Hygino H. Domingues

FUNDAMENTOS DE ARITMÉTICA

Dados de Catalogação na Publicação (CIP) Internacional
(Câmara Brasileira do Livro, SP, Brasil)

Domingues, Hygino H., 1934-

Fundamentos de aritmética / Hygino H. Domingues. — São Paulo : Atual, 1991.
Fundamentos de aritmética / Hygino H. Domingues. — São Paulo : Atual, 1991.

ISBN 85-7056-342-6

1. Aritmética I. Título.

91-0448 CDD-513

Índices para catálogo sistemático:

1. Aritmética 513

Fundamentos de aritmética

Editora: Bárbara Ferreira Arena
Assistente editorial: Sandra Lucia Abrano
Chefe de preparação e revisão de texto: Noé Ribeiro
Preparadora de texto: Maria Luiza Simões
Revisores: Maria de Lourdes Chaves Ferreira
Paulo Sá
Chefe de arte: Zildo Braz
Gerente de produção: Antonio Cabello Q. Filho
Produção gráfica: Silvia Regina E. Almeida (coord.)
José Rogerio L. de Simone
Assessoria técnica: Gil Marcos Ferreira
Capa: Sylvio Ulhôa Cintra Filho
Projeto gráfico: Sonia Regina Vaz
Composição e arte-final: Diarte Editora e Com. de Livros Ltda.
Fotolito: Binhos
Impressão: F.C.A.

ATUAL EDITORA LTDA.
Rua José Antônio Coelho, 785
04011 — São Paulo — SP

ISBN 85-7056-342-6

NOS PEDIDOS TELEGRÁFICOS BASTA CITAR O CÓDIGO ADRM 1021 A

PREFÁCIO

O presente texto corresponde, de alguma maneira, a uma idealização do curso de *Teoria dos Números* (60 h/a) que tivemos ocasião de ministrar algumas vezes na graduação em Matemática da Unesp, campus de São José do Rio Preto. Imaginamos um curso com carga horária maior, no qual a aritmética fosse desenvolvida inicialmente para os números naturais e depois estendida para os inteiros, em sintonia com sua evolução histórica. E, aproveitando o material teórico assim criado, construir ao fim a teoria da representação decimal dos números reais.

O capítulo I é uma introdução histórica à aritmética, obviamente despretensiosa. Acreditamos que se justifique tal capítulo não só pela proposta do livro mas também pelas ligações quase orgânicas entre as origens da matemática e da aritmética. A teoria dos números propriamente dita, objeto central do texto, figura nos capítulos II e III, mas não ultrapassa o âmbito do elementar e do básico sobre o assunto. O estudo da forma decimal aparece nos capítulos IV e V sobre números racionais e reais, respectivamente.

Ao longo de todos os capítulos houve a preocupação de tornar o texto auto-suficiente. Com esse objetivo, fomos desde a construção dos campos numéricos até alguns detalhes sobre convergência no corpo ordenado dos números reais. Mas, para não tornar o texto demasiadamente pesado, no que se refere a estes aspectos às vezes omitimos justificativas e às vezes recorremos à intuição geométrica.

Assim, esperamos apresentar um texto que seja útil, especialmente sob o aspecto didático, para professores e estudantes de matemática (inclusive em nível do segundo grau). Aliás, uma outra preocupação nossa foi explicar o porquê de certos procedimentos e algoritmos usados desde muito cedo no ensino da matemática mas de uma maneira puramente mecânica.

E não poderíamos encerrar sem o registro de nossos agradecimentos especiais: aos editores, em particular ao Prof. Gelson Iezzi, pela confiança demonstrada no convite para redigirmos este trabalho; à Profª Ermínia de Lourdes Campello Fanti, pela atenciosa leitura que fez da primeira redação dos capítulos II a V (teoria) e pelas oportunas sugestões então apresentadas.

O autor

Dedicado a meus filhos:

Renata
Regina
Renan

SUMÁRIO

CAPÍTULO I

NÚMEROS, SISTEMAS DE NUMERAÇÃO: INTRODUÇÃO HISTÓRICA

1. Origens

Em algum momento da história a Aritmética tem início com o homem começando a contar e, por conseqüência, a associar números (ainda que implicitamente) a coleções de objetos e seres que o rodeavam. Mas quando, onde e mesmo de que maneira, são indagações para cuja resposta não há como fugir a hipóteses e conjecturas.

Na verdade é difícil imaginar que alguma civilização de antepassados nossos, mesmo a mais primitiva, não tivesse entre seus valores culturais, não importa quão limitados fossem estes, pelo menos o embrião da idéia de número. Discernir entre um e dois, por exemplo, é algo que mesmo culturas muito atrasadas com certeza conseguiram atingir. Essa impressão, aliás, é confirmada pela antropologia, através do estudo de culturas primitivas que remanesceram até nossa época. Como algumas tribos aborígines da Austrália capazes apenas de contar até dois, quantificando qualquer coleção com mais de um par de elementos simplesmente por "muitos".

Assim é que nossos antepassados, talvez há uns 30 000 anos, começaram a se preocupar com o registro quantitativo de entes e coisas ligados à sua vida tribal: os familiares, cabeças de gado, dias que se passaram desde um certo evento, etc. E de que procedimento lançaram mão para levar a efeito esse registro? É bastante provável que isso fosse feito através da idéia de correspondência biunívoca. Ou seja, a cada elemento do conjunto a ser quantificado associava-se uma marca ou algum elemento de outro conjunto (mais fácil de ter junto a si e de manipular), o qual passava então a servir de referência.

Por exemplo, os dedos das mãos e, se necessário, os dos pés, poderiam ser usados sem dificuldades para indicação de quantos membros tinha uma família. Mas caso se tratasse de um clã ou de um rebanho, a coleção de todos os dedos de um indivíduo poderia ser insuficiente. Para conferir um rebanho, nas suas idas e vindas do pastoreio, um expediente bastante provável consistiria em formar um monte de pedrinhas, uma para cada cabeça de gado que

saía de manhã; e no seu regresso, ao fim da tarde, uma pedrinha seria retirada do monte para cada animal que voltasse. Mas é claro que também um monte de pedras está muito longe do ideal para um registro quantitativo.

Em 1937 Karl Absolom encontrou na Tchecoslováquia uma tíbia de lobo de aproximadamente 7 polegadas de comprimento, datando de cerca de 30 000 anos, na qual estão gravados 55 cortes transversais, em grupos de 5, sendo que os 25 primeiros se acham separados dos demais por um par de cortes maiores.

É claro que não seria improcedente conjecturar que cada um dos cortes corresponde a algum objeto ou ser de um conjunto, familiar ao homem pré-histórico que os fez, visando a ter dele uma avaliação quantitativa. A cada elemento da coleção (de peles, parentes ou cabeças de gado, por exemplo) era feito um único corte sobre o osso. Essa é uma outra forma do uso da idéia de correspondência biunívoca.

E como explicar a divisão dos cortes em grupos de 5 e, depois, uma divisão maior a fim de formar de 5 grupos de 5 cortes um grupo maior? É razoável supor que por trás desse fato esteja também o embrião de outra das idéias fundamentais da Matemática, ou seja, a de base de um sistema de numeração — no caso base 5.

Assim, cada cinco unidades simples formavam uma unidade de ordem imediatamente superior e cinco destas últimas formavam uma unidade da ordem seguinte. Se essa era a idéia usada, sem dúvida estaríamos diante de um exemplo de emprego da base 5. Mas é claro que apenas esse achado arqueológico, apesar de sua importância, não permite nenhuma conclusão definitiva.

A evolução do conceito de contagem e de número, a partir dessa fase, foi muito lenta e em etapas difíceis de determinar. Por exemplo, o que teria vindo primeiro: o uso de símbolos gráficos ou o uso de arranjos de sons para designar um número? A hipótese mais plausível, até pelas dificuldades subjacentes a cada um desses avanços, é a de que primeiro teriam surgido os símbolos. De qualquer maneira pode ter ocorrido a princípio que um mesmo símbolo ou o mesmo arranjo de sons designasse indistintamente, por exemplo, "dez carneiros" e "dez cabras". Só bem depois, talvez, é que foram surgindo símbolos ou arranjos de sons distintos para cada uma dessas situações.

Em todo o caso, a culminância desse processo, diga-se de passagem bastante recente na história do homem, é a dos números como abstrações, em que os símbolos e arranjos de sons usados para indicá-los passam a ter um significado que independe de qualquer possível associação com particulares coleções de objetos ou seres. Hoje, por exemplo, a simples enunciação de "dez" já desperta em quem a ouve ou lê uma idéia quantitativa muito clara que não depende de qualquer outra referência.

As primeiras culturas a usar símbolos especiais para designar números localizaram-se junto aos vales dos rios Nilo, Tigre e Eufrates, Indo e Yangtse Kiang (China) e remontam a cerca de 6 000 anos.

2. Sistemas de numeração

Se dois conjuntos finitos e não vazios podem ser colocados em *correspondência biunívoca*, ou seja, se a cada elemento do primeiro é possível associar, de alguma maneira, um único elemento do segundo, e vice-versa, então há entre esses conjuntos, sob o aspecto quantitativo, algo em comum. Diz-se que ambos têm o mesmo *número* de elementos ou a mesma *cardinalidade*. Os símbolos usados para indicar os números chamam-se *numerais*.

Com o desenvolvimento de uma sociedade vai-se tornando necessário contar conjuntos cada vez mais numerosos, efetuar cálculos, o que ficaria muito difícil sem uma sistematização do processo de contagem e, paralelamente, do procedimento para escrever os números. O expediente de que o homem fez uso nesse sentido, desde tempos imemoriais, foi, como já mencionamos de passagem, a escolha de uma base para formar grupos de elementos.

Esquematicamente, a idéia de base pode assim ser explicada: um certo número natural $b > 1$ é escolhido como base; isso significa que um agrupamento de b unidades simples (de primeira ordem) forma uma unidade de segunda ordem, um agrupamento de b unidades de segunda ordem forma uma unidade de terceira ordem, e assim por diante (no nosso sistema, por exemplo, dez unidades formam uma *dezena*, dez dezenas uma *centena*, dez centenas um *milhar*, etc.); são atribuídos nomes e símbolos especiais para $1, 2, \ldots, b$ (ou $0, 1, 2, \ldots, b - 1$, se o zero é conhecido) e, às vezes, para $b^2, b^3, \ldots$; os nomes e símbolos para os demais números são construídos a partir daqueles já introduzidos, mediante regras convenientes.

Por que esta ou aquela base? Certamente isso depende, de algum modo, do conjunto tomado como referência em relação ao qual todos os demais são avaliados. A propósito dos sistemas de base 10 (como o que usamos, por exemplo, Aristóteles observou que essa escolha decorre do acidente anatômico de termos dez dedos nas mãos. É curioso observar que o vocábulo dígito, hoje usado para indicar qualquer dos algarismos de 0 a 9, é originário do termo latino *digitus*, que significa dedo.

3. Alguns sistemas de numeração

a) Os egípcios desenvolveram um sistema de numeração hieroglífico de base 10 há cerca de 5 000 anos. Esse sistema usava símbolos diferentes para os números $1, 10, 10^2, 10^3, \ldots$

1 = |	1 000 = 𓆼	(flor de lótus)
10 = ∩	10 000 = 𓂭	(dedo com a ponta curvada)
100 = 𓍢	100 000 = 𓆐	(girino)

A escrita de um número se baseava no princípio da adição dos valores dos símbolos (princípio *aditivo*). Por exemplo:

3 = |||
26 = ∩∩ ||| |||
105 = 𓍢 ||| ||

b) Mais ou menos na mesma época em que os egípcios desenvolveram seu sistema de numeração hieroglífico, surgia na Mesopotâmia um sistema com a mesma estrutura que o nosso atual — porém de base 60. Tal como o que usamos hoje em dia, esse sistema era *posicional*, ou seja, o valor dos símbolos usados dependia de sua posição na escrita do número, o que explicaremos em pouco.
Mas por que base 60? Não há uma resposta taxativa a essa pergunta mas, provavelmente, essa escolha foi conseqüência do fato de 60 unidades admitirem várias subdivisões: em metades, terços, quartos, quintos, sextos, décimos, doze avos, quinze avos, vigésimos e trigésimos. Isso era muito importante numa região onde a Matemática estava fortemente ligada a atividades comerciais.
Contudo o sistema de numeração babilônico (como costuma ser chamado) era incompleto na medida em que usava dois símbolos apenas:

1 = 𒁹 e 𒌋 = 10

Assim, até o número 59 era um sistema aditivo. Por exemplo:

6 = 𒁹𒁹𒁹 𒁹𒁹𒁹 21 = 𒌋𒌋 𒁹

Daí para a frente entrava a idéia de base 60 e o princípio posicional. Por exemplo:

𒁹 𒌋𒁹 𒁹𒁹𒁹 $= 3 + 11 \cdot 60 + 1 \cdot 60^2 = 4\,263$

Ou seja, o símbolo 𒁹𒁹𒁹, por ocupar a primeira posição (da direita para a esquerda), valia efetivamente 3; o 𒌋𒁹, por ocupar a segunda posição, valia $11 \cdot 60 = 660$; o 𒁹, por ocupar a terceira posição, valia $1 \cdot 60^2 = 3\,600$.
O fato de não haver um símbolo para indicar o zero, além de a escrita babilônica ser feita em plaquetas de argila, não raro tornava ambígua a leitura de um numeral. Por exemplo: 𒁹𒁹
tanto podia representar o 2, como 61 ou 120, além de outros números.

c) Os gregos antigos usaram dois sistemas de numeração. O mais recente, o jônico, era também um sistema de base 10, aditivo, mas com algumas particularidades interessantes. Os símbolos do sistema eram 27: as 24 letras do alfabeto grego e mais 3 letras em desuso. Os gregos também não trabalhavam com o zero. Os valores eram associados às letras da seguinte maneira:

1 = α; 2 = β; 3 = γ; ...; 8 = η; 9 = θ
10 = ι; 20 = κ; 30 = λ; ...; 80 = π; 90 = ϙ
100 = ρ; 200 = σ; 300 = τ; ...; 800 = ω; 900 = ϡ

Nesse quadro as letras em desuso eram ϙ (koppa), ϡ (sampi) e ϛ (vaù) = 6. Com esses símbolos e mais o uso de um acento, como explicaremos a seguir, era possível expressar qualquer número inferior a 10 000 com quatro letras apenas (uma eventualmente acentuada), o que não deixa de ser uma vantagem.
Por exemplo:

12 = ιβ; 23 = κγ; 382 = τπβ

Para os nove primeiros múltiplos de 1 000 utilizavam as nove primeiras letras da tabela anterior precedidas de um acento, como no exemplo a seguir:

‘θ = 9 000; ‘θσιγ = 9 213

E quando se tratava de escrever os números a partir de 10 000 usavam o princípio da multiplicação, colocando sobre a letra maiúscula M (mu) ou à sua direita os símbolos convenientes de 1 a 9 999. Por exemplo:

$\overset{\gamma}{M} = 30\,000$; $\overset{\rho\lambda}{M} = 1\,300\,000$

Um sistema como o jônico é chamado às vezes de *sistema de numeração cifrado*.

d) O sistema de numeração romano (ainda com alguns usos hoje em dia) é também decimal aditivo. Os símbolos para 1, 10, 10^2 e 10^3 são, respectivamente, I, X, C e M. Mas há também símbolos especiais para 5 = V, 50 = L e 500 = D, o que torna mais breve a expressão de um número. Por exemplo, ao invés de justapor sete vezes o símbolo I para indicar o 7, basta escrever VII. Também por uma questão de brevidade o sistema incorporou, ao longo do tempo, um princípio subtrativo:

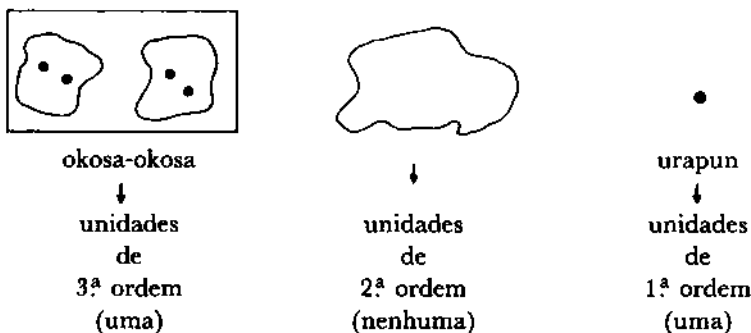
IV = 5 − 1; IX = 10 − 1; XC = 100 − 10; CM = 1 000 − 100

Assim, se um romano da época de Cristo escrevia

1 989 = MDCCCCLXXXVIIII

já pelos fins da idade média o mais comum era

1 989 = MCMLXXXIX

e) O uso da base 2 é comum hoje em computação eletrônica. Mas o que é uma opção técnica dos nossos dias foi prática espontânea de muitos povos. Algumas dezenas de tribos de índios norte-americanos, por exemplo, adotavam a base 2.
Uma delas, do oeste americano do século passado, embora sem possuir uma linguagem escrita, e embora discernindo os números apenas até o seis, contava da seguinte maneira: 1, "urapun"; 2, "okosa"; 3, "okosa-urapun"; 4, "okosa-okosa"; 5, "okosa-okosa-urapun"; 6, "okosa-okosa-okosa"; mais do que 6, "ras". O número 5, por exemplo, pode ser decomposto da seguinte maneira:

f) No capítulo II (item 5) mostraremos que, uma vez escolhido um número natural $b > 1$, todo número natural *a* pode ser representado, de maneira única, do seguinte modo:

$$a = a_r b^r + a_{r-1} b^{r-1} + \ldots + a_1 b + a_0$$

onde $r \geqslant 0$ e $0 \leqslant a_0, a_1, \ldots, a_r < b$. Em virtude desse fato, a correspondência que associa a cada número natural *a* a seqüência $(a_r\, a_{r-1} \ldots a_1\, a_0)_b$ é bijetora, o que permite representar o número através da seqüência.
Essa notação, e os elementos teóricos em que se baseia, caracterizam o que se chama *sistema de numeração posicional*. Para escrever qualquer número são necessários b símbolos, um para o zero, outro para a unidade, outro para duas unidades, ..., e um para $b - 1$ unidades. Esses símbolos são chamados dígitos.

Na expressão $(a_r\, a_{r-1} \ldots a_1\, a_0)_b$ os símbolos $a_0, a_1, \ldots, a_r$ representam respectivamente as unidades de primeira, segunda, ..., $(r - 1)$-ésima ordem. Na verdade o valor de a_1 é $a_1 b$, o de a_2 é $a_2 b^2$, etc.
No caso da base 10 (nosso sistema de numeração) omitem-se os parênteses e o índice. Os dígitos, como se sabe, são 0, 1, 2, ..., 9. Por exemplo:

$$179 = 9 + 7 \cdot 10 + 1 \cdot 10^2$$

4. O nascimento da teoria dos números

4.1 Antecedentes

No item anterior focalizamos o sistema de numeração hieroglífico egípcio e o sistema de numeração usado na Mesopotâmia. É interessante observar que tanto os egípcios como os babilônios construíram, ao longo de sua história, um acervo matemático significativo. Desenvolveram a aritmética, a geometria e a álgebra, até um certo ponto. Mas essa matemática, apesar de suficiente para embasar algumas realizações materiais importantes desses povos, e apesar de exibir alguns vislumbres teóricos, tinha limitações sérias sob o ponto de vista científico.

De um lado porque a matemática desses povos pouco passava de uma coleção de conclusões empíricas a que chegaram ao longo dos séculos. E sendo quase um receituário, não se cogitava de conceitos teóricos e muito menos de possíveis deduções lógicas. Outro ponto que obstava seriamente o desenvolvimento da matemática de egípcios e babilônios era sua quase total ausência de abstração. No caso de números e operações numéricas, se pensavam abstratamente talvez nem se dessem conta disso. Mas em geometria, por exemplo, para eles com certeza uma reta não passava de uma corda esticada e um retângulo nada mais era do que uma cerca ou algo equivalente. Em que pesem suas raízes empíricas e sua múltipla aplicabilidade, a Matemática é uma ciência dedutiva e, portanto, só como tal pode se desenvolver plenamente.

Mas uma nova atitude em relação à Matemática teria lugar na Grécia Antiga, mais ou menos a partir do século VI a.C. Na verdade os gregos mudaram a relação do homem com o universo à medida que, embora sem desprezar totalmente a observação e a experimentação, passaram a adotar a razão como o grande instrumento na busca da verdade. No que tange à Matemática, essa postura se consubstanciou na grande ênfase dada ao método dedutivo a partir de axiomas enunciados *a priori*. Outro ponto importante é que a primeira fase da matemática grega, que vai mais ou menos do século VI a.C. à morte de Alexandre, o Grande, em 323 a.C., se desenvolveu junto a escolas filosóficas,

resultando daí algumas de suas diretrizes básicas como, por exemplo, a organização lógica e o caráter abstrato de que se revestiu.

O primeiro matemático grego de nomeada foi Tales de Mileto (séc. VI a.C.), também filósofo. Pouco se sabe sobre a vida e a obra de Tales, mas não foi com ele ainda que a matemática grega atingiu o caráter abstrato e o rigor lógico que vieram a caracterizá-la. Talvez tenha sido ele o primeiro indivíduo na história a formular algumas propriedades gerais sobre figuras geométricas. Por exemplo: "Os ângulos da base de um triângulo isósceles são iguais entre si". Com formulações como essa, desvinculadas de exemplos concretos, começa a nascer a geometria como ciência.

4.2 A escola pitagórica

Pitágoras nasceu na ilha de Samos por volta do ano 560 a.C. Quando jovem visitou demoradamente o Egito, a Índia e a Mesopotâmia, onde, a par da Matemática, certamente absorveu muito do misticismo desses lugares.

Com cerca de 40 anos de idade fixou-se em Crotona, colônia grega situada ao sul da Itália, e lá fundou um misto de escola e comunidade religiosa em que coexistiam o cultivo da Filosofia, da Ciência e da Matemática, com a devoção e o ascetismo, em meio a uma vida comunitária e mística. Os ensinamentos eram transmitidos oralmente e sob promessa de segredo (é possível que não houvesse essa exigência com relação à Matemática). Era norma da escola atribuir todas as descobertas realizadas por seus membros ao chefe — daí não se poder discernir hoje entre as contribuições de Pitágoras e as de seus discípulos ou seguidores. De qualquer maneira nenhum documento original restou sobre a matemática pitagórica que, apesar de toda a influência que exerceu, só é conhecida através de fontes indiretas, referências ou informações esparsas.

Com o tempo a ordem pitagórica acabou se envolvendo na política local, o que provocou a expulsão de seu líder da cidade de Crotona. Pitágoras encontrou refúgio em Metaponto, cidade grega situada no golfo de Tarento, também na Itália, onde morreu no ano 497 a.C. Mas a escola continuou a existir por pelo menos mais dois séculos e, dentre os sucessores de Pitágoras, os mais preeminentes foram Filolaus (450-365 a.C.) e Arquitas de Tarento (428-347 a.C.). Foi através de um livro escrito por Filolaus que as doutrinas pitagóricas foram reveladas, quebrando o silêncio e o mistério de cerca de um século que havia em torno delas. Platão (428-328 a.C.), que inclusive foi amigo de Arquitas, teve acesso à obra de Filolaus. Dessa forma, e também através dos sofistas, a matemática pitagórica entrou em Atenas, onde exerceu grande influência.

A atitude de tentar explicar o universo racionalmente (o que não significa necessariamente de maneira correta) começou com os gregos. Para Tales,

por exemplo, a água era o princípio fundamental de todas as coisas. Os pitagóricos encontraram nos números (para eles apenas os naturais não nulos) e nas relações numéricas a chave para a explicação do universo. Aristóteles (384-322 a.C.) afirma, em sua *Metafísica*, que para os pitagóricos os números eram a componente última dos objetos reais e materiais. Fatos percebidos por eles, como as ligações da Matemática com a astronomia e a música, por exemplo, devem tê-los levado a tal concepção.

Mas deve-se levar em conta que para os primeiros pitagóricos os números certamente não eram entes abstratos, como os concebemos hoje. Nessa primeira fase com certeza os imaginavam concretamente, de alguma maneira constituídos de pontos materiais — o que explica, pelo menos em parte, a posição que ocupavam em sua filosofia.

Isso contudo deve ter mudado com o correr do tempo. Segundo Proclus (410-485 d.C.) em seu *Comentário* ao livro primeiro dos *Elementos*, de Euclides — muito provavelmente baseado numa "história" da Matemática de Eudemo de Rodes (séc. IV a.C.), uma obra que se perdeu de então para cá —, a matemática pura foi uma criação dos pitagóricos, o que é bem provável.

4.3 A aritmética pitagórica

Não resta dúvida que os pitagóricos viam o papel dos números no mundo de uma maneira muito especial. Daí não ser surpresa que a aritmética teórica tenha nascido entre eles. Como a escola tratava a matemática de maneira muito filosófica e abstrata, desvinculada das exigências da vida prática, era natural que separassem o estudo teórico dos números, que chamavam "aritmética", dos cálculos práticos, que denominavam "logística", preocupando-se essencialmente apenas com o primeiro desses aspectos. É curioso observar que hoje em dia, entre nós, a chamada aritmética corresponde muitas vezes à logística dos gregos antigos. Mas o termo aritmética vem do grego e suas raízes são as seguintes: *arithmos*, que significa número, e *technes*, que se traduz por ciência.

Aos pitagóricos se deve a distinção entre números pares e ímpares. Os seguintes teoremas, entre outros, eram conhecidos por eles:

a) A soma de dois números pares é par.
b) O produto de dois números ímpares é ímpar.
c) Quando um número ímpar divide um número par, também divide sua metade.

Muita coisa da matemática pitagórica foi reunida nos *Elementos*, de Euclides (c. 300 a.C.), uma obra em treze livros, abarcando a Matemática elementar da época. Os livros VII, VIII e IX são exatamente sobre aritmética teórica, porém, como era praxe entre os gregos da época, o enfoque e a lingua-

gem são geométricos. Por exemplo, a definição 5 do livro VII diz o seguinte: "Um número é parte de outro, o menor do maior, quando ele mede o maior". Era assim que Euclides expressava que um número era divisor de um outro (maior que ele).

Dividiam também os números em *primos* e *secundários* (compostos). A definição 11 do livro VII citado é a seguinte: "Um número primo é aquele que é mensurável apenas pela unidade". Mensurável aí, obviamente, significa divisível. Nessas condições o próprio 1 poderia ser considerado primo não fosse ele excluído do rol dos números (naturais, não nulos), por ser o gerador de todos. Mesmo o 2 às vezes não era considerado primo, por ser o gerador dos pares. Mas Aristóteles dizia que o 2 é "o único número par primo".

Outro conceito que também aparece nos *Elementos* e que provavelmente remonta aos pitagóricos é o de *número perfeito*: "Número perfeito é aquele que é igual à soma de suas partes". Por exemplo, 6 é perfeito pois $6 = 1 + 2 + 3$. Note-se que eles interpretavam "parte" de um número como um *divisor próprio* do número, isto é, um divisor diferente do próprio número. O número 28 também é perfeito já que $28 = 1 + 2 + 4 + 7 + 14$. No capítulo II (item 9.2) voltaremos ao assunto com mais detalhes.

Também se atribui aos pitagóricos a descoberta dos *números amigáveis*. Dois números se dizem amigáveis se cada um deles é a soma dos divisores próprios do outro, como ocorre com 220 e 284, pois:

soma dos divisores próprios de $220 = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$

e

soma dos divisores próprios de $284 = 1 + 2 + 4 + 71 + 142 = 220$

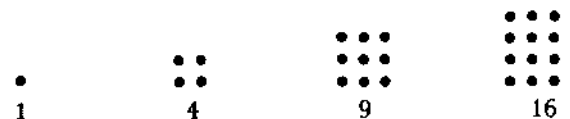
4.4 Os números figurados

Na época de Pitágoras ainda se contava através do uso de pedrinhas ou de marcas de pontos na areia. Por outro lado eram os pitagóricos observadores atentos de formas geométricas. Daí porque, talvez, tiveram sua atenção chamada para os *números figurados*. Estes, como diz o próprio nome, resultam de arranjos com pontos ou pedrinhas de maneira a formar figuras geométricas.

Assim, os números 1, 3, 6, 10, ... são chamados *triangulares* porque correspondem à distribuição de pedrinhas num plano na forma de triângulos, do seguinte modo:

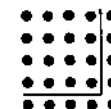
Se indicarmos por T_n o enésimo número triangular, vale a fórmula:

$$T_n = 1 + 2 + \ldots + n = \frac{1}{2}\, n(n+1)$$

Os números que resultam de dispor pedrinhas num plano de modo a formar quadrados, conforme figura a seguir, chamam-se *números quadrados*:

Muitos resultados interessantes sobre números figurados podem ser obtidos de maneira puramente geométrica e informal. Indicando por Q_n o enésimo número quadrangular e dividindo seus pontos como na figura

observa-se que

$$Q_n = T_{n-1} + T_n = \frac{1}{2}\,(n-1)n + \frac{1}{2}\, n(n+1) = \frac{1}{2}\, n(2n) = n^2$$

Para passar de um número quadrangular a outro os pitagóricos procediam segundo o esquema

de onde sai

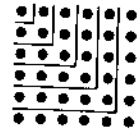
$$Q_n + (2n+1) = Q_{n+1}$$

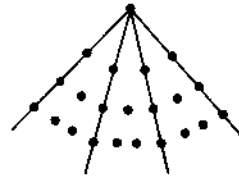
ou seja

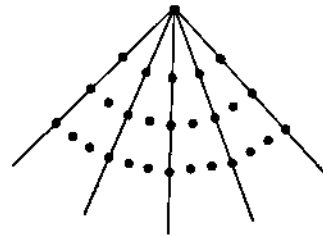
$$n^2 + (2n+1) = (n+1)^2$$

uma identidade elementar bastante conhecida.

O conjunto de pontos à direita e abaixo do ângulo reto traçado na figura anterior era chamado *gnômon*.

Outra propriedade interessante ligada aos números quadrados pode ser obtida da figura a seguir:

$$1 + 3 + 5 + \ldots + (2n - 1) = n^2$$

Números pentagonais:

$1, 5, 12, 22, \ldots, P_n, \ldots$

Números hexagonais:

$1, 6, 15, 28, \ldots, H_n, \ldots$

Nessa maneira de representar os números figurados, os gnômons são sempre, em cada etapa, os pontos que ficam na poligonal, que fecham a figura na parte inferior. Ademais, cada segmento dessa linha poligonal tem um ponto a mais que o correspondente da poligonal anterior. Como no caso dos números hexagonais são quatro os segmentos de cada gnômon, então a diferença entre o número de pontos de dois gnômons consecutivos é 4. Para os números eneagonais essa diferença é $n - 2$.

Assim, no caso dos números hexagonais, os sucessivos gnômons têm

$$1 + 4 = 5, \ 5 + 4 = 9, \ 9 + 4 = 13, \ \ldots, \ 4n + 1, \ \ldots$$

pontos. Logo:

$$H_n = 1 + 5 + 9 + \ldots + [4(n - 1) + 1] = \frac{(1 + 4n - 3) \cdot n}{2} = 2n^2 - n$$

4.5 Os ternos pitagóricos

Hoje em dia são conhecidas algumas centenas de demonstrações do chamado teorema de Pitágoras, segundo o qual o quadrado da hipotenusa de um triângulo retângulo é igual à soma dos quadrados dos catetos. Embora já conhecido antes de Pitágoras, é bem possível contudo que se deva a ele, ou à sua escola, a primeira demonstração dessa relação fundamental da geometria métrica.

Mas, considerando o grau de preocupação dos pitagóricos no sentido de ligar os números (naturais) às coisas, especialmente à geometria, era natural esperar que procurassem determinar todos os triângulos retângulos de lados inteiros. Este problema consiste em resolver no conjunto dos ternos ordenados de números naturais não nulos a equação $x^2 + y^2 = z^2$. Um terno (a, b, c) de números naturais não nulos tal que $a^2 + b^2 = c^2$ chama-se *terno pitagórico*.

Com isso a escola pitagórica inaugurou o estudo de problemas indeterminados envolvendo números naturais, algo que seria retomado posteriormente, com grande fôlego, por Diofanto de Alexandria (séc. III, d.C.). Embora a solução geral para essa questão só viesse a aparecer nos *Elementos*, os pitagóricos deram sua contribuição ao assunto.

Talvez observando que o gnômon que fecha o número n^2 tem $2n + 1$ pontos e que este número corresponde a dois lados de um quadrado

os pitagóricos devem ter experimentado fazer $2n + 1 = m^2$. Daí segue que

$$n = \frac{m^2 - 1}{2}$$

e portanto:

$$n + 1 = \frac{m^2 + 1}{2}$$

Como $(n + 1)^2 = n^2 + 2n + 1$, então:

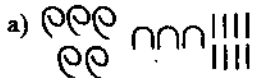
$$\left(\frac{m^2+1}{2}\right)^2 = \left(\frac{m^2-1}{2}\right)^2 + (m^2-1) + 1$$

Donde

$$\left(\frac{m^2+1}{2}\right)^2 = \left(\frac{m^2-1}{2}\right)^2 + m^2$$

Logo, se m é um número ímpar (se o quadrado de um número natural é ímpar, o próprio número também o é), então

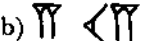
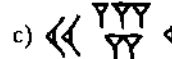
$$\left(m, \frac{m^2-1}{2}, \frac{m^2+1}{2}\right) \quad (*)$$

é um terno pitagórico. Por exemplo, para m = 3 obtém-se (3, 4, 5) e para m = 5 obtém-se (5, 12, 13), ambos pitagóricos. Mas o terno (8, 15, 17) é obviamente pitagórico mas não se enquadra em (*). Voltaremos ao assunto, para completá-lo, no item 10 do capítulo II.

EXERCÍCIOS

1. Escreva cada um dos seguintes números em hieróglifos egípcios:

a) 1 493
b) 641
c) 6 548
d) 15 127

2. Passe cada um dos seguintes numerais egípcios para o nosso sistema de numeração:

a)
b)
c)

3. Expresse em notação babilônica os seguintes números:

a) 1 000
b) 1 342
c) 10 000
d) 12 348

4. Passe para o nosso sistema de numeração:

a)
b)
c)
d)

5. Um dos vestígios deixados pelo sistema de numeração sexagesimal da Mesopotâmia é o sistema de medida de ângulos em graus, minutos e segundos (sessenta segundos valem um minuto e sessenta minutos valem um grau). Isto posto, efetue:

a) 10°42'23'' + 36°38'44''
b) 21°10'15'' − 10°11'32''
c) 3 × (45°38'43'')
d) (42°20'6'') : 6

6. Escreva os numerais jônicos gregos correspondentes a:

a) 398
b) 1 223
c) 9 128
d) 20 392

7. Passe do sistema de numeração jônico grego para o nosso sistema de numeração:

a) τπα
b) σϙη
c) M'βσιθ (com α sobre M)
d) M τλγ (com λ sobre M)

8. Para efetuar uma multiplicação, como 26 × 54, por exemplo, os gregos procediam segundo a decomposição a seguir:

$$26 \times 54 = (20 + 6) \cdot (50 + 4) =$$
$$= 20 \cdot 50 + 20 \cdot 4 + 6 \cdot 50 + 6 \cdot 4$$
$$= 1\ 404$$

O dispositivo prático, ainda usando nossos numerais, era o seguinte:

```
      26
    × 54
  ---------
  1 000  80
    300  24
  ---------
  1 300 104 = 1 404
```

Em numerais jônicos, observando que $4 = \delta$, $50 = \nu$ e $400 = \upsilon$ (upsilon):

$$\begin{array}{rr} \kappa & \varsigma \\ \nu & \delta \\ \hline {}^{\prime}\alpha & \pi \\ \tau & \kappa\delta \\ \hline {}^{\prime}\alpha\ \tau & \varrho\delta \end{array} = {}^{\prime}\alpha\upsilon\delta$$

Efetue, segundo o método jônico, a multiplicação de $\lambda\gamma$ (= 33) por $\pi\alpha$ (= 81). Use $40 = \mu$ (mu), $70 = o$ (omicron) e $600 = \chi$ (chi).

9. No sistema de numeração romano uma barra sobre um certo numeral multiplica seu valor por 1 000, ao passo que duas barras o multiplicam por $1\ 000^2$. Assim:

$$\overline{\text{IV}} = 4\ 000 \qquad \text{e} \qquad \overline{\overline{\text{XV}}} = 15\ 000\ 000$$

Escreva os numerais romanos correspondentes a:

a) 1 492
b) 1 998
c) 74 812
d) 3 142 236

10. Passe para o nosso sistema de numeração os seguintes numerais romanos:

a) CXXIV
b) MDCCXLVIII
c) $\overline{\text{XIX}}$
d) $\overline{\overline{\text{XC}}}\text{XXV}$

11. Mostre que são perfeitos os números 496 e 8 128.

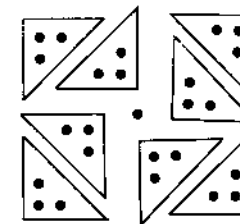
12. Mostre que os números 1 184 e 1 210 são amigáveis.

Nota: A descoberta de que esses dois números são amigáveis só foi feita em 1886 por um jovem italiano de 16 anos de idade chamado Nicolo Paganini.

13. Plutarco (c. 100 d.C.) afirmou que se um número triangular é multiplicado por 8 e acrescido de 1 o resultado é um número quadrado. Prove este fato e faça uma ilustração geométrica dele.

Resolução: Como $T_n = \dfrac{n(n+1)}{2}$, então

$$8T_n + 1 = 4n(n+1) + 1 = 4n^2 + 4n + 1 = (2n+1)^2 = Q_{2n+1}$$

Uma ilustração geométrica para o caso n = 2 pode ser vista na figura a seguir.

14. Prove que o quadrado de qualquer número ímpar, múltiplo de 3, é a diferença entre dois números triangulares.

15. Prove que $P_n = T_{n-1} + Q_n$, para todo $n \geqslant 1$.

16. Escreva os seguintes números como soma de no máximo três números triangulares:

a) 56
b) 69
c) 287

17. Estabeleça a seguinte fórmula para todo $n \geqslant 1$:

$(2n+1)^2 = (4T_n + 1)^2 - (4T_n)^2$.

18. Mostre que 1 225 e 41 616 são, simultaneamente, números triangulares e quadrados.

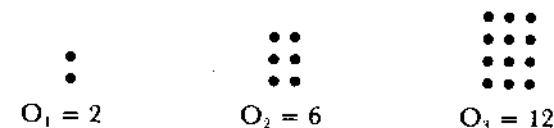
Resolução: Obviamente 1 225 é número quadrado, pois $1\ 225 = 35^2$. Por outro lado, de

$$\frac{n(n+1)}{2} = 1\ 225$$

segue que $n^2 + n - 2\ 450 = 0$ e portanto (resolvendo esta equação) $n = 99$. Assim:

$$1\ 225 = T_{99} = Q_{35}$$

19. Um *número oblongo* conta a quantidade de pontos sobre um plano de maneira a formar um retângulo em que o número de linhas é uma unidade maior que o de colunas. Se O_n indica o enésimo número oblongo, então

$O_1 = 2$ $O_2 = 6$ $O_3 = 12$

e, em geral, $O_n = n(n+1)$.

Prove algébrica e geometricamente que:

a) $O_n = 2 + 4 + \ldots + 2n$

b) Todo número oblongo é a soma de dois números triangulares iguais.

c) $O_n + n^2 = T_{2n}$

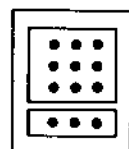
d) $O_n - n^2 = n$

e) $n^2 + 2O_n + (n + 1)^2 = (2n + 1)^2$

f) $O_n = 1 + 2 + \ldots + n + (n + 1) + (n - 1) + (n - 2) + \ldots + 3 + 2$

Resolução:

a) $2 + 4 + \ldots + 2n = \dfrac{(2 + 2n)n}{2} = n(n + 1) = O_n$

b) No caso $n = 3$:

$$O_3 = T_3 + T_3$$

Em geral: $O_n = T_n + T_n$

c) $O_n + n^2 = n(n + 1) + n = n(2n + 1) = \dfrac{2n(2n + 1)}{2} = T_{2n}$

d)

$$O_n = n^2 + n$$

20. Prove a seguinte fórmula para a soma dos n primeiros números triangulares, estabelecida pelo matemático indiano Aryabhatta (c. 500 d.C.):

$$T_1 + T_2 + \ldots + T_n = \frac{n(n + 1)(n + 2)}{6}$$

Sugestão: Agrupe o primeiro membro em pares e substitua cada soma $T_{k-1} + T_k$ por k^2 (considere o caso n par e o caso n ímpar).

CAPÍTULO II

OS NÚMEROS NATURAIS

1. Introdução

O objetivo deste capítulo é fazer um estudo aritmético do conjunto $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ dos números naturais. Um pré-requisito para este assunto seria, num enfoque mais formal e completo, a própria construção lógica de $\mathbb{N}$. Mas isto só será feito, e mesmo assim omitindo-se alguns detalhes, no Apêndice I, ao fim do capítulo. Obviamente esta abordagem significa que, embora a ênfase seja a aritmética propriamente dita, não queremos deixar de chamar a atenção para seus princípios básicos — algo cuja necessidade passa muitas vezes totalmente despercebida.

Enquanto a geometria, 300 anos antes de Cristo, nos *Elementos* de Euclides, já recebia um tratamento lógico-dedutivo, com seus postulados e axiomas, definições e teoremas, para a teoria dos números (e mesmo para as demais partes da matemática) demorou muito um tratamento semelhante.

A primeira tentativa nesse sentido se deve a Giovanni Campano (viveu por volta de 1260). Este capelão do Papa Urbano IV procurou fundamentar os números naturais em 4 postulados, o último dos quais afirmava que "um número não pode diminuir indefinidamente", o que significa, no fundo, a existência do mínimo de qualquer coleção de números naturais. Posteriormente Gottfried W. Leibniz (1646-1716) assinalou que "verdades" tão evidentes como 2 + 2 = 4 devem ser objeto de demonstração a partir do conceito de número, o mesmo devendo acontecer também com propriedades aparentemente tão óbvias como a comutativa da adição e a comutativa da multiplicação. Mas Leibniz não se alongou no assunto.

Mas ao se chegar ao século XIX já não era possível à Matemática, no estágio que atingira e no ritmo em que se desenvolvia, continuar se apoiando quase que inteiramente na intuição. E seus alicerces passaram a ser investigados amplamente e a receber a fundamentação lógica necessária.

No que se refere aos números, parece que a primeira tentativa séria nesse sentido foi feita por Hermann G. Grassmann (1809-1877) que, em 1861, definiu adição e multiplicação de inteiros e demonstrou as propriedades fundamentais dessas operações, usando apenas a função sucessor $x \to x + 1$ e implicitamente o princípio de indução. O primeiro sistema completo de axiomas para a aritmética foi apresentado por Richard Dedekind (1831-1916) em 1888. A axiomática que formularemos no Apêndice I se deve a Giuseppe Peano (1858-1932) e data de 1891.

2. Operações — relação de ordem

Não faremos aqui, como já foi dito, a construção lógica de $\mathbb{N} = \{0, 1, 2, \ldots\}$. Tampouco serão dadas agora as definições formais de adição e multiplicação de números naturais. O leitor interessado encontrará tudo isso no já citado Apêndice I. Neste parágrafo nos limitaremos a citar as propriedades dessas duas operações que servem de embasamento teórico à aritmética dos números naturais. Antes disso registremos que o conjunto $\mathbb{N} - \{0\}$ será indicado pela notação $\mathbb{N}^*$. Ou seja: $\mathbb{N}^* = \{1, 2, 3, \ldots\}$.

2.1 Adição

a_1 $a + (b + c) = (a + b) + c$, $\forall a, b, c \in \mathbb{N}$ (associativa)
a_2 $a + b = b + a$, $\forall a, b \in \mathbb{N}$ (comutativa)
a_3 $a + 0 = a$, $\forall a \in \mathbb{N}$ (0 é o elemento neutro da adição em $\mathbb{N}$)
a_4 $a + b = a + c \Rightarrow b = c$ (lei do cancelamento da adição)

2.2 Multiplicação

m_1 $a(bc) = (ab)c$, $\forall a, b, c \in \mathbb{N}$ (associativa)
m_2 $ab = ba$, $\forall a, b \in \mathbb{N}$ (comutativa)
m_3 $a \cdot 1 = a$, $\forall a \in \mathbb{N}$ (1 é o elemento neutro da multiplicação)
m_4 $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (lei do anulamento do produto)
m_5 $(ac = bc$ e $c \neq 0) \Rightarrow a = b$ (lei do cancelamento da multiplicação)
m_6 $ab = 1 \Rightarrow a = 1$ e $b = 1$
m_7 $a(b + c) = ab + ac$, $\forall a, b, c \in \mathbb{N}$ (a multiplicação é distributiva em relação à adição)

Nota: O símbolo $\Rightarrow$ será sempre usado neste texto com o significado de "se..., então...". Por exemplo a propriedade m_6 deve ser interpretada da

maneira condicional seguinte: "Se a e b são números naturais e $ab = 1$, então $a = 1$ e $b = 1$". E o símbolo $\Longleftrightarrow$ será empregado com o sentido de "se, e somente se".

2.3 Relação de ordem

Define-se a relação $\leqslant$ (menor que ou igual) em $\mathbb{N}$ do seguinte modo: se $a, b \in \mathbb{N}$, diz-se que $a \leqslant b$ se $b = a + u$, para algum $u \in \mathbb{N}$. O número u nessas condições chama-se *diferença* entre b e a e é indicado por $u = b - a$, onde b é o *minuendo* e a o *subtraendo*.

Assim a *subtração* $(a, b) \to a - b$ só está definida neste caso para os pares ordenados (a, b) em que $a \geqslant b$. Valem as seguintes propriedades:

- $(b - a) + a = b$, sempre que $a \leqslant b$
  De fato, se $b - a = u$, então $b = a + u = a + (b - a)$
- Se $c \leqslant a$, então $(a + b) - c = (a - c) + b$
  Seja $a - c = u$. Então $a = c + u$ e portanto $a + b = c + (u + b)$. Donde $(a + b) - c = u + b = (a - c) + b$
  Do mesmo modo se provam:
- $b + c \leqslant a \Rightarrow a - (b + c) = (a - b) - c$
  Neste caso simplifica-se a notação assim:
  $(a - b) - c = a - b - c$
- Se $b \leqslant a$ e $d \leqslant c$, então $(a - b) + (c - d) = (a + c) - (b + d)$.

Mas vejamos agora as principais propriedades da relação $\leqslant$. Observemos antes que algumas delas poderiam ser provadas a partir dos resultados que já temos, ao passo que a demonstração de outras depende de pré-requisitos que figuram no Apêndice I.

O_1 $a \leqslant a$, $\forall a \in \mathbb{N}$ (reflexiva)
O_2 $a \leqslant b$ e $b \leqslant a \Rightarrow a = b$ (anti-simétrica)
O_3 $a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$ (transitiva)
O_4 $a \leqslant b$ ou $b \leqslant a$ (a relação $\leqslant$ é total)
O_5 $a \leqslant b \Rightarrow a + c \leqslant b + c$, $\forall c \in \mathbb{N}$ ($\leqslant$ é compatível com a adição)
O_6 $a \leqslant b \Rightarrow ac \leqslant bc$, $\forall c \in \mathbb{N}$ ($\leqslant$ é compatível com a multiplicação)

Por valerem as seis propriedades anteriores diz-se que $\leqslant$ é uma relação de ordem total sobre $\mathbb{N}$ compatível com a adição e a multiplicação de $\mathbb{N}$.

Diz-se que a é *menor que* b e escreve-se $a < b$ se $b = a + v$, para algum $v \neq 0$. É claro então que: $a < b \Longleftrightarrow a \leqslant b$ e $a \neq b$

O_7 $a < b \Rightarrow a + 1 \leqslant b$
O_8 Se L é um subconjunto não vazio de $\mathbb{N}$, então L possui um elemento m tal que $m \leqslant x$ para todo $x \in L$ (*princípio do menor número natural*).

O elemento m que aparece em O_8 é chamado *mínimo* de L e será indicado por m = min L. É fácil provar que m é único. De fato, se m_1 = min L, então $m \leqslant m_1$ (pois $m_1 \in L$) e $m_1 \leqslant m$ (pois m_1 = min L e $m \in L$). Logo $m = m_1$. Por exemplo, o mínimo do conjunto $\{1, 3, 5, 7, \ldots\}$ é 1

Dado $L \subset \mathbb{N}$, $L \neq \emptyset$, um elemento $M \in L$ (caso exista) tal que $x \leqslant M$, $\forall x \in L$, chama-se *máximo* de L. Notação: M = max L. Se L possui máximo, este é único (demonstração análoga à que se fez para o mínimo). Há subconjuntos não vazios de $\mathbb{N}$ que não têm máximo: é o caso de $\{1, 3, 5, \ldots\}$ e $\{0, 2, 4, 6, \ldots\}$, por exemplo.

Alternativamente poderemos usar $b \geqslant a$ com o significado de $a \leqslant b$ e $b > a$ com o de $a < b$.

As propriedades a seguir decorrem do que já vimos e, vez por outra, são necessárias:

- $a \leqslant b$ e $b < c \Rightarrow a < c$
- $a < b \Rightarrow a + c < b + c$
- $a + c \leqslant b + c \Rightarrow a \leqslant b$
- $(a \leqslant b$ e $c \leqslant d) \Rightarrow a + c \leqslant b + d$
- $(a < b$ e $c \neq 0) \Rightarrow ac < bc$
- $(a < b$ e $c \leqslant d) \Rightarrow a + c < b + d$
- $c \leqslant b \Rightarrow a(b - c) = ab - ac$

3. Indução

3.1 Primeiro princípio de indução

Apesar da designação clássica, trata-se de uma proposição relativamente fácil de provar a partir dos resultados que já temos. Eis o seu enunciado:

"Seja $a \in \mathbb{N}$ e suponhamos que a cada número natural $n \geqslant a$ esteja associada uma afirmação $P_{(n)}$. Admitamos ainda que seja possível provar o seguinte:

i $P_{(a)}$ é verdadeira

ii Para todo $r \geqslant a$, se $P_{(r)}$ é verdadeira, então $P_{(r+1)}$ também é verdadeira.

Então $P_{(n)}$ é verdadeira para todo $n \geqslant a$."

A idéia da demonstração é simples. Devido a **i** $P_{(a)}$ é verdadeira. De **ii** segue então que $P_{(a+1)}$ é verdadeira. Ainda por **ii** decorre que $P_{(a+2)}$ é verdadeira. E assim por diante.

Vejamos como formalizar esse raciocínio.

Demonstração: Seja $L = \{x \in \mathbb{N} | x \geqslant a$ e $P_{(x)}$ é falsa$\}$. Basta provar então que $L = \emptyset$. Suponhamos $L \neq \emptyset$ e seja m = min L. Logo $P_{(m)}$ é falsa e como, por hipótese, $P_{(a)}$ é verdadeira, então $m > a$. Desta última relação segue que $m > 0$; portanto $m = 1 + u$, para algum $u \in \mathbb{N}$, e daí $u < m$.

Mas $m > a$ implica que $m \geqslant a + 1$. Assim $m = 1 + u \geqslant a + 1$, do que resulta $u \geqslant a$.

Em resumo: $m > u \geqslant a$. Mas isto obriga $P_{(u)}$ a ser verdadeira (se fosse falsa, u estaria em L, o que não é possível pois $u < m$ = min L). Então, devido a **ii**: $P_{(u+1)} = P_{(m)}$ é verdadeira. Absurdo. ■

A afirmação $P_{(r)}$ que figura em **ii**, no enunciado do princípio, é chamada *hipótese de indução*.

3.2 Somatórios e produtórios em $\mathbb{N}$

São comuns em Matemática as *definições por recorrência* (*recursão*). Na verdade trata-se de definições por indução.

Examinemos o caso da adição e o da multiplicação em $\mathbb{N}$. Sendo ambas operações binárias sobre $\mathbb{N}$, a soma e o produto de dois números naturais estão naturalmente definidos. Admitindo que também o estejam para $n - 1 \geqslant 2$ números quaisquer de $\mathbb{N}$ e pondo, por definição

$$a_1 + a_2 + \ldots + a_n = (a_1 + \ldots + a_{n-1}) + a_n$$

e

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n$$

então passa a ter sentido falar em soma ou produto de $m \geqslant 2$ naturais quaisquer.

Assim, por exemplo:

$$a_1 + a_2 + a_3 = (a_1 + a_2) + a_3$$
$$a_1 + a_2 + a_3 + a_4 = (a_1 + a_2 + a_3) + a_4$$

Faremos uso, como é praxe, das seguintes notações:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$$

onde o primeiro membro deve ser lido "somatório dos a_i, para i de 1 a n" e

$$\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n$$

cujo primeiro membro se lê "produtório dos a_i, para i de 1 a n".

Quando n = 1 faz-se, por extensão:

$$\sum_{i=1}^{n} a_i = a_1 \qquad e \qquad \prod_{i=1}^{n} a_i = a_1$$

Outro conceito que pode ser introduzido por recorrência é o de *potência n-ésima de a*, onde a, n ∈ IN, a ≠ 0. Por definição:

$a^0 = 1$
$a^{n+1} = a^n \cdot a$, sempre que $n \geq 0$.

Isto significa que $a^1 = a^0 \cdot a = 1 \cdot a = a$, $a^2 = a^1 \cdot a = a \cdot a$, $a^3 = a^2 \cdot a = (a \cdot a) \cdot a$, e assim por diante.

Exemplo 1: Provemos por indução sobre n que $a^m \cdot a^n = a^{m+n}$, para quaisquer m, n ∈ IN, sempre que a ≠ 0.

$$n = 0 : a^m \cdot a^0 = a^m \cdot 1 = a^m = a^{m+0}$$

Logo, a propriedade vale para n = 0.
Hipótese de indução: $a^m \cdot a^r = a^{m+r}$, ∀r ≥ 0.

$$n = r + 1 : a^m \cdot a^{r+1} = a^m \cdot (a^r \cdot a) = (a^m \cdot a^r) \cdot a \overset{(*)}{=} a^{m+r} \cdot a = a^{(m+r)+1} = a^{m+(r+1)}.$$

Note-se que a hipótese de indução foi usada na passagem (*).

A definição de potência pode ser estendida a a = 0 do seguinte modo: $0^n = 0$, para todo n ∈ IN, n ≠ 0.

Se a é um número natural e existe b ∈ IN de modo que $a = b^2$, então se diz que a é um *quadrado perfeito*. Os números naturais quadrados perfeitos são: 0, 1, 4, 9, 16, ..., n^2, ... E se $a = b^3$ para algum b ∈ IN, então a é chamado *cubo perfeito*. Os cubos perfeitos são: 0, 1, 8, 27, ..., n^3, ...

Exercício: Se a ∈ IN, a ≠ 0, prove que $(a^m)^n = a^{mn}$, ∀m, n ∈ IN (use indução sobre n).

PROPRIEDADES Vejamos agora algumas propriedades básicas envolvendo somatórios e produtórios:

i $$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n \qquad e$$

$$\prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n \qquad (\forall n \geq 2)$$

A validade destas propriedades é decorrência imediata dos conceitos e notações nelas envolvidos.

ii $$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \qquad e$$

$$\prod_{i=1}^{n} (a_i b_i) = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} b_i\right)$$

Provemos por indução a primeira dessas relações (indução sobre n).

$$n = 1 : \sum_{i=1}^{n} (a_i + b_i) = a_1 + b_1;\ \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = a_1 + b_1$$

Vamos supor a propriedade válida para r ≥ 1. Então:

$$\sum_{i=1}^{r+1} (a_i + b_i) = \left[\sum_{i=1}^{r} (a_i + b_i)\right] + (a_{r+1} + b_{r+1}) =$$
$$= \left(\sum_{i=1}^{r} a_i + \sum_{i=1}^{r} b_i\right) + (a_{r+1} + b_{r+1}) =$$
$$= \left[\left(\sum_{i=1}^{r} a_i\right) + a_{r+1}\right] + \left[\left(\sum_{i=1}^{r} b_i\right) + b_{r+1}\right] =$$
$$= \sum_{i=1}^{r+1} a_i + \sum_{i=1}^{r+1} b_i$$

iii Para todo k ∈ IN: $\sum_{i=1}^{n} (ka_i) = k \sum_{i=1}^{n} a_i$ e $\prod_{i=1}^{n} (ka_i) = k^n \prod_{i=1}^{n} a_i$.

A demonstração fica como exercício (indução sobre n).

iv Se $a_i = a$ (i = 1, 2, ..., n), então:

$$\sum_{i=1}^{n} a_i = na \qquad e \qquad \prod_{i=1}^{n} a_i = a^n$$

Provemos a segunda dessas propriedades por indução sobre n.

$$n = 1 : \prod_{i=1}^{n} a_i = a_1 = a \qquad e \qquad a^n = a^1 = a$$

Seja r ≥ 1 e suponhamos $\prod_{i=1}^{r} a_i = a^r$

Então $\prod_{i=1}^{r+1} a_i = \left(\prod_{i=1}^{r} a_i\right)a_{r+1} = a^r \cdot a = a^{r+1}$

v Se $a_i = i$ ($i = 1, 2, \ldots, n$), então:

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Vamos também por indução sobre n.

$n = 1$: $\sum_{i=1}^{n} a_i = a_1 = 1$ e $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1$

Admitamos $r \geqslant 1$ e $\sum_{i=1}^{r} i = \frac{r(r+1)}{2}$

Então:

$$\sum_{i=1}^{r+1} a_i = \left(\sum_{i=1}^{r} a_i\right) + a_{r+1} = \frac{r(r+1)}{2} + (r+1) = \frac{r(r+1) + 2(r+1)}{2} =$$

$$= \frac{(r+1)(r+2)}{2}$$

Por exemplo:

$$\sum_{i=1}^{5} (3i+2) = 3\sum_{i=1}^{5} i + \sum_{i=1}^{5} 2 = 3 \cdot \frac{5(5+1)}{2} + 5 \cdot 2 = 55$$

$$\prod_{i=1}^{4} (i+2)^2 = \left[\prod_{i=1}^{4} (i+2)\right]^2 = (3 \cdot 4 \cdot 5 \cdot 6)^2 = 129\,600$$

vi Somatórios duplos

Sejam $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n \in \mathbb{N}$ ($m \geqslant 1$, $n \geqslant 1$). Às vezes há necessidade de considerar a soma de todos os produtos possíveis $a_i b_j$ ($1 \leqslant i \leqslant m$; $1 \leqslant j \leqslant n$). Mas esses produtos são exatamente as parcelas de:

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = (a_1 + \ldots + a_i + \ldots + a_m)(b_1 + \ldots + b_j + \ldots + b_n)$$

Assim, em virtude de iii, deste item,

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i\right)b_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i b_j\right)$$

e, analogamente:

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_i b_j\right)$$

Em vista desse resultado a soma de todos os $a_i b_j$ é usualmente indicada por:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j \quad \text{ou} \quad \sum_{j=1}^{n}\sum_{i=1}^{m} a_i b_j$$

Estas expressões recebem o nome de *somatórios duplos*. Das considerações feitas resulta que:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = \left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right)$$

Por exemplo:

a) $\sum_{i=1}^{2}\sum_{j=1}^{3} (2i)(3+j) = \left(\sum_{i=1}^{2} 2i\right)\left(\sum_{j=1}^{3} (3+j)\right) =$

$= \left(2\sum_{i=1}^{2} i\right)\left(\sum_{j=1}^{3} 3 + \sum_{j=1}^{3} j\right) =$

$= 2 \cdot \frac{2 \cdot 3}{2} \cdot \left(3 \cdot 3 + \frac{3 \cdot 4}{2}\right) = 6 \cdot (9+6) = 90$

b) $\sum_{i=1}^{3}\sum_{j=1}^{2} i^2 \cdot 2^j = \left(\sum_{i=1}^{3} i^2\right)\left(\sum_{j=1}^{2} 2^j\right) =$

$= (1+4+9) \cdot (2+4+8) = 14 \cdot 14 = 196$

c) Se $m = n$, então:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} ij = \left(\sum_{i=1}^{n} i\right)\left(\sum_{j=1}^{n} j\right) = \left(\sum_{i=1}^{n} i\right)^2 = \left[\frac{n(n+1)}{2}\right]^2$$

Nota: Se $a_1, a_2, \ldots, a_n \in \mathbb{N}$ ($n \geqslant 1$) e $1 \leqslant r \leqslant n$, pomos, por definição:

$$\sum_{i=r}^{n} a_i = a_r + a_{r+1} + \ldots + a_n$$

e

$$\prod_{i=r}^{n} a_i = a_r a_{r+1} \ldots a_n$$

Assim, para $n \geqslant 2$ e $1 \leqslant r < n$:

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{r} a_i + \sum_{i=r+1}^{n} a_i$$

e

$$\prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{r} a_i\right)\left(\prod_{i=r+1}^{n} a_i\right)$$

3.3 Segundo princípio de indução

Seja $a \in \mathbb{N}$ e suponhamos que a cada natural $n \geqslant a$ esteja associada uma afirmação $P_{(n)}$. Admitamos ainda que seja possível provar as duas condições seguintes:

i $P_{(a)}$ é verdadeira.
ii Para todo $r > a$, se $P_{(k)}$ é verdadeira sempre que $a \leqslant k < r$, então $P_{(r)}$ também é verdadeira.

Então $P_{(n)}$ é verdadeira para todo $n \geqslant a$.

A demonstração deste princípio, aliás muito parecida com a do anterior, fica como exercício. Teremos ocasião, ainda neste capítulo, de usar algumas vezes este princípio.

EXERCÍCIOS

21. Calcule:

a) $\sum_{i=1}^{4} (2i + 3)$

b) $\sum_{i=2}^{4} i(i + 2)$

c) $\sum_{i=1}^{r+2} 3i$

d) $\sum_{i=1}^{3} 2^i$

22. Calcule:

a) $\prod_{i=1}^{4} 5$

b) $\prod_{i=1}^{3} i^2$

c) $\prod_{i=2}^{5} (i + 2)(i + 3)$

d) $\prod_{i=2}^{4} 3^i$

23. Escreva, usando o símbolo de somatório ou produtório:

a) $(a_1 + 2) + (a_2 + 4) + (a_3 + 4)$

b) $2^3 + 3^4 + 4^5 + \ldots + n^{n+1}$

c) $7 \cdot 8 \cdot 9 \cdot 10 \ldots 25$

d) $a_1b_2 + a_2b_3 + \ldots + a_nb_{n+1}$

e) $1^2 + 2^2 + \ldots + n^2$

f) $2^1 + 2^2 + 2^3 + \ldots + 2^p$

24. (Fuvest-81) P é uma propriedade relativa aos números naturais. Sabe-se que: 1) P é verdadeira para o natural $n = 10$; 2) Se P é verdadeira para n, então P é verdadeira para 2n; 3) Se P é verdadeira para n, $n \geqslant 2$, então P é verdadeira para $n - 2$. Pode-se concluir que:

a) P é verdadeira para todo natural n.
b) P é verdadeira somente para os números naturais n, $n \geqslant 10$
c) P é verdadeira para todos os números naturais pares.
d) P é verdadeira somente para as potências de 2.
e) P não é verdadeira para os números ímpares.

25. Prove por indução:

a) $1^2 + 2^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$ $(n \geqslant 1)$

b) $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$ $(n \geqslant 1)$

c) $1 \cdot 2 + 2 \cdot 3 + \ldots + n \cdot (n+1) = \dfrac{n(n+1)(n+2)}{3}$ $(n \geqslant 1)$

d) $a \geqslant 1 \Rightarrow a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$ $(n \geqslant 1)$

e) $2n \leqslant n^2$ $(n \geqslant 2)$

f) $a \geqslant 2 \Rightarrow 2a^n \leqslant a^{n+1}$ $(n \geqslant 1)$

g) $a \geqslant 1 \Rightarrow a^{n+1} \leqslant a^{2n}$ $(n \geqslant 1)$

h) $a \geqslant 2 \Rightarrow 1 + a + \ldots + a^n < a^{n+1}$ $(n \geqslant 1)$

i) $n^3 < n!$ $(n \geqslant 6)$

j) $n! > n^2$ $(n \geqslant 4)$

Resolução de h):

Para $n = 1$ a relação é $1 + a < a^2$ que obviamente é verdadeira para $a = 2$. Supondo $1 + k < k^2$ $(k \geqslant 2)$, então $1 + (k + 1) = (1 + k) + 1 < k^2 + 1 < k^2 + 2k + 1 = (k + 1)^2$. Logo $1 + a < a^2$, para todo $a \geqslant 2$.
Seja $r \geqslant 1$ e façamos a hipótese

$$1 + a + \ldots + a^r < a^{r+1}$$

Daí

$$1 + a + \ldots + a^r + a^{r+1} < a^{r+1} + a^{r+1} = 2a^{r+1} \leq a^{r+2}$$

o que conclui a resolução. Note-se que na última passagem usamos o resultado proposto em f).

26. Prove que:

$$1 + 3 + \ldots + (2n - 1) = n^2$$

ou seja, que a soma dos n primeiros números ímpares é n^2.

27. Prove por indução sobre n que o número de subconjuntos de um conjunto finito com n elementos é 2^n.

28. Prove por indução sobre n que:

$$(a^m)^n = a^{mn}$$

para quaisquer $a, m, n \in \mathbb{N}$, $a \neq 0$.

29. Se $b + c \leq a$, mostre que:

$$a - (b + c) = (a - b) - c$$

30. Sejam $x, y \in \mathbb{N}$. Se $3 < x < 6$ e $6 < y < 10$, mostre que $2 \leq y - x \leq 5$. De um modo geral, prove que se $a < x < b$ e $b < y < c$, então $2 \leq y - x \leq c - a - 2$.

31. Prove que o produto de quatro *números naturais consecutivos*, acrescido de 1, é um quadrado perfeito.

Resolução: Se a indica o menor dos números, então os outros são $a + 1$, $a + 2$ e $a + 3$.
Como

$$a(a + 1)(a + 2)(a + 3) = a^4 + 6a^3 + 11a^2 + 6a$$

deve-se procurar $m \in \mathbb{N}$ de modo que:

$$a^4 + 6a^3 + 11a^2 + 6a + 1 = (a^2 + ma + 1)^2$$

Desenvolvendo o segundo membro e identificando o resultado com o primeiro, obtém-se $m = 3$. Logo:

$$1 + a(a + 1)(a + 2)(a + 3) = (a^2 + 3a + 1)^2$$

Por exemplo, se $a = 4$, então:

$$1 + 4 \cdot 5 \cdot 6 \cdot 7 = (4^2 + 12 + 1)^2 = 29^2$$

4. Divisibilidade em IN

4.1 Múltiplos e divisores

DEFINIÇÃO 1 Diz-se que um número natural a *divide* um número natural b se $b = ac$, para algum $c \in \mathbb{N}$. Neste caso diz-se também que a é *divisor* de b e que b é *múltiplo* de a. Ou ainda que b é *divisível* por a. Indicaremos por $a \mid b$ o fato de a dividir b; e se a não divide b, escrevemos $a \nmid b$.

O elemento $c \in \mathbb{N}$ tal que $b = ac$, onde $a \neq 0$, é indicado por $c = \frac{b}{a}$ ou, eventualmente, por $c = b : a$ e é chamado quociente de b por a.

Por exemplo, $2 \mid 6$ pois $6 = 2 \cdot 3$, $5 \mid 10$ pois $10 = 5 \cdot 2$, $1 \mid a$ ($\forall a \in \mathbb{N}$) pois $a = 1 \cdot a$ e $0 \mid 0$ uma vez que $0 = 0 \cdot a$, para todo $a \in \mathbb{N}$. Mas, se $b \neq 0$, então $0 \nmid b$ pois $0 \cdot c = 0 \neq b$, $\forall c \in \mathbb{N}$.

Atenção: Não se deve confundir o símbolo | com o traço de fração ——. Assim, $2 \mid 6$ (p. ex.) não deve ser confundido com $\frac{2}{6}$ ou $\frac{6}{2}$. Enquanto estes dois últimos símbolos indicam numerais, $2 \mid 6$ expressa uma relação particular entre 2 e 6. O que ocorre é que, conforme notação já introduzida, $2 \mid 6$ equivale a $6 = 2 \cdot \frac{6}{2}$. Assim, $0 \mid 0$ é uma relação verdadeira, ao passo que $\frac{0}{0}$ é uma expressão indeterminada.

Para a relação $x \mid y$ em IN valem as seguintes propriedades:

d_1 $a \mid a$, $\forall a \in \mathbb{N}$, pois $a = a \cdot 1$ (reflexiva)

d_2 $a \mid b$ e $b \mid a \Rightarrow a = b$ (anti-simétrica)
De fato, por hipótese, $b = ac$ e $a = bd$. Daí: $a = a(cd)$. Se $a = 0$, como $b = ac$, então $b = 0$. Se $a \neq 0$, então $cd = 1$ e portanto $c = d = 1$. Logo $a = b$ também neste caso.

d_3 $a \mid b$ e $b \mid c \Rightarrow a \mid c$ (transitiva)
Como $b = ar$ e $c = bs$, então $c = a(rs)$

d_4 Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, $\forall x, y \in \mathbb{N}$
Em particular: $a \mid b \Rightarrow a \mid bx$, $\forall x \in \mathbb{N}$
De $b = ar$ e $c = as$ (hipóteses) decorre que $bx = arx$ e $cy = asy$. Donde $bx + cy = arx + asy = a(rx + sy)$.

Nota: Do que vimos segue que: $a \mid b$ e $a \mid c \Rightarrow a \mid (b + c)$. Além disso,

$$\frac{b + c}{a} = \frac{b}{a} + \frac{c}{a}$$

pois:

$$\left(\frac{b}{a} + \frac{c}{a}\right)a = \frac{b}{a} \cdot a + \frac{c}{a} \cdot a = b + c$$

$\mathbf{d_5}$ Se $c|a$, $c|b$ e $a \leqslant b$, então $c|(b-a)$.
Por hipótese $a = cr$ e $b = cs$. Fazendo $b = a + u$, então $cs = cr + u$ e daí $u = cs - cr = c(s - r)$. Logo $c|u$ e como $u = b - a$ a propriedade está provada. Neste caso:

$$\frac{b-a}{c} = \frac{b}{c} - \frac{a}{c}$$

$\mathbf{d_6}$ Seja $a = b + c$ e suponhamos $d|b$. Então: $d|a \iff d|c$. $(c = a - b)$
$(\Rightarrow)$ é $\mathbf{d_5}$ e $(\Leftarrow)$ é $\mathbf{d_4}$ para $x = y = 1$.

$\mathbf{d_7}$ Se $a|b$ e $b \neq 0$, então $a \leqslant b$.
Das hipóteses segue que existe $q \in \mathbb{N}^*$ de modo que $b = aq$. Como $q > 0$, então, devido a $\mathbf{O_7}$, $1 = 0 + 1 \leqslant q$ e portanto $q = 1 + u$, para algum $u \in \mathbb{N}$. Daí $b = aq = a(1 + u) = a + au$, o que implica $a \leqslant b$.

Notação: Indicaremos por M_a o conjunto dos múltiplos de a. Assim $M_a = \{0, a, 2a, 3a, \ldots\}$. Em particular $M_0 = \{0\}$ e $M_1 = \mathbb{N}$. Os elementos de $M_2 = \{0, 2, 4, \ldots\}$ são chamados *números naturais pares* e os de $\mathbb{N} - M_2 = \{1, 3, 5, \ldots\}$ de *naturais ímpares*.

4.2 O algoritmo da divisão (ou de Euclides)

Seja b um número natural não nulo. Se $a \in \mathbb{N}$, então ou a é múltiplo de b ou está entre dois *múltiplos consecutivos* de b, isto é: $bq \leqslant a < b(q + 1)$. Isto significa que $q + 1$ é o mínimo de $\{n \in \mathbb{N} \mid bn > a\}$, subconjunto não vazio de $\mathbb{N}$ pois contém o elemento $a + 1$. (De fato: $b \geqslant 1 \Rightarrow ab \geqslant a \Rightarrow ab + b \geqslant a + b \Rightarrow b(a + 1) \geqslant a + b > a$.)

De $bq \leqslant a$ resulta que existe $r \in \mathbb{N}$ tal que $a = bq + r$. Mostremos que $r < b$. Se $r = a - bq \geqslant b$, então $(a - bq) + bq \geqslant b + bq$ e daí $a \geqslant b(q + 1)$, o que não é possível. Assim:

$$a = bq + r \ (r < b)$$

As considerações que acabamos de fazer podem assim ser sintetizadas:
"Dados $a, b \in \mathbb{N}$, $b \neq 0$, existem $q, r \in \mathbb{N}$ de maneira que $a = bq + r$ $(r < b)$".

Obviamente, se $r = 0$, então a é múltiplo de b.

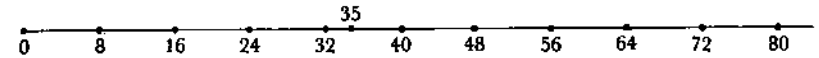
Suponhamos $a = bq + r = bq_1 + r_1$, onde $r < b$ e $r_1 < b$. Admitamos que se pudesse ter $r \neq r_1$, digamos $0 < r - r_1 < b$ (já levando em conta que tanto r como r_1 são menores que b). Mas então da igualdade $bq + r = bq_1 + r_1$ decorre que $bq + (r - r_1) = bq_1$ e portanto $b|(r - r_1)$. Donde $b \leqslant r - r_1$, o que é absurdo. Logo $r = r_1$ e portanto $q = q_1$.

Provamos pois o

TEOREMA 1 *(algoritmo da divisão ou de Euclides):* "Para quaisquer a, $b \in \mathbb{N}$, $b \neq 0$, existe um único par de números q e r, de maneira que $a = bq + r$ $(r < b)$".

Os elementos a, b, q e r são chamados, respectivamente, *divisor*, *dividendo*, *quociente* e *resto* da divisão de a por b.

Exemplo 2: Vamos aplicar o algoritmo aos números $a = 35$ e $b = 8$. Observemos que 35 está entre os múltiplos 32 e 40 de 8:

35
0 8 16 24 32 40 48 56 64 72 80

$8 \cdot 4 < 35 < 8 \cdot (4 + 1)$. Logo $q = 4$ e $r = 35 - 8 \cdot 4 = 3$. Isso explica o algoritmo

$$\begin{array}{r|l} 35 & 8 \\ \hline -32 & 4 \\ \hline 3 & \end{array}$$

Exemplo 3: Procuraremos explicar agora o algoritmo usual prático da divisão, calculando o quociente e o resto quando $a = 351$ e $b = 8$. Numa primeira etapa, quando se faz

$$\begin{array}{r|l} 351 & 8 \\ \hline 31 & 4 \end{array}$$

na verdade o 4 que aparece sob a chave não passa do algarismo das dezenas do quociente procurado, como se pode verificar a seguir:

$35 = 8 \cdot 4 + 3$ (algoritmo da divisão para 35 e 8) $\Rightarrow$
$\Rightarrow 350 = 8 \cdot 40 + 30$
$\Rightarrow 351 = 8 \cdot 40 + 31$

Usando agora o algoritmo com os números 31 e 8:

$$31 = 8 \cdot 3 + 7$$

Logo

$$351 = 8 \cdot 40 + 8 \cdot 3 + 7 = 8 \cdot 43 + 7$$

Voltando ao dispositivo prático:

$$\begin{array}{r|l} 351 & 8 \\ \hline 31 & 43 \\ 7 & \end{array}$$

5. Sistemas de numeração posicionais — base

Em nosso sistema de numeração todo número n é um polinômio

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$$

onde $r \geqslant 0$ e os $a_i \in \{0, 1, 2, \ldots, 9\}$ $(i = 1, 2, \ldots, r)$ estão univocamente determinados. O numeral que representa n é escrito assim:

$$a_r a_{r-1} \ldots a_1 a_0$$

Por exemplo:

$$641 = 1 + 4 \cdot 10 + 6 \cdot 10^2$$

Mas o papel desempenhado pelo 10 em nosso sistema de numeração é apenas uma opção ou uma circunstância, como mostra o resultado a seguir.

TEOREMA 2 Seja b um número natural maior que 1 e seja $M = \{0, 1, 2, \ldots, b - 1\}$. Então todo número n pode ser representado univocamente da seguinte maneira:

$$n = a_0 + a_1 \cdot b + a_2 \cdot b^2 + \ldots + a_r \cdot b^r$$

onde $r \geqslant 0$, $a_i \in M$ $(i = 1, 2, \ldots, r)$ e $a_r \neq 0$.

Demonstração:

i A existência será provada por indução (segundo princípio) sobre n. Se $n < b$, então $n = n$ é a representação pretendida. Vamos tomar $n \geqslant b$ e admitir como hipótese que para todo q, $1 \leqslant q < n$, essa representação seja possível. Aplicando o algoritmo da divisão para n e b se obtém

$$n = bq + a_0 \ (a_0 \in M)$$

Note-se que não pode ocorrer $q \geqslant n$. De fato, como $b > 1$, então $bq > q$ e essa hipótese levaria a $bq > n$ e portanto a $bq + a_0 = n > n$. Logo $1 \leqslant q < n$ e pela hipótese de indução:

$$q = a_1 + a_2 b + \ldots + a_r b^{r-1} \ (a_i \in M;\ a_r \neq 0)$$

Conseqüentemente,

$$n = b(a_1 + a_2 b + \ldots + a_r b^{r-1}) + a_0 = a_0 + a_1 b + a_2 b^2 + \ldots + a_r b^r$$

conforme o enunciado.

ii A unicidade também será provada por indução sobre n e é trivial para $n < b$. Seja $n \geqslant b$ e suponhamos que a unicidade se verifique para todo q, $1 \leqslant q < n$. Suponhamos ainda que:

$$n = a_0 + a_1 b + \ldots + a_r b^r = a'_0 + a'_1 b + \ldots + a'_s b^s$$

onde, também, $a'_0, a'_1, \ldots, a'_s \in M$. Então:

$$n = b(a_1 + a_2 b + \ldots + a_r b^{r-1}) + a_0 =$$
$$b(a'_1 + a'_2 b + \ldots + a'_s b^{s-1}) + a'_0$$

Como $b > a_0$ e $b > a'_0$, o algoritmo de Euclides (unicidade) garante que $a_0 = a'_0$ e $a_1 + a_2 b + \ldots + a_r b^{r-1} = a'_1 + a'_2 b + \ldots + a'_s b^s = q$. Como $q < n$, então, pela hipótese de indução, $r - 1 = s - 1$ (do que segue $r = s$) e $a_1 = a'_1, a_2 = a'_2, \ldots, a_r = a'_r$. ■

Se cada um dos elementos do conjunto $M = \{0, 1, \ldots, b - 1\}$ é representado por um símbolo especial, então cada um desses símbolos é chamado *algarismo* do *sistema posicional de base b*. A proposição demonstrada torna válido representar cada número $n = a_0 + a_1 b + \ldots + a_r b^r$ pela seqüência dos algarismos que nele figuram da seguinte maneira:

$$n = (a_r a_{r-1} \ldots a_2 a_1)_b$$

No caso $b = 10$ omitem-se os parênteses e o índice.

Quando $1 < b \leqslant 10$ é praxe usar os próprios algarismos indo-arábicos que sejam necessários para indicar os dígitos de 0 a $b - 1$. **Por exemplo**:

$$(2102)_3 = 2 + 0 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 = 65$$
$$(10001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 = 17$$

Exemplo 4: Dado um número n escrito na base 10, a demonstração da proposição anterior (primeira parte) mostra como passá-lo para uma base b qualquer. Por exemplo, consideremos $n = 4\,761$ e $b = 8$. Apliquemos o algoritmo da divisão a 4 761 e 8:

$$4\,761 = 8 \cdot 595 + 1$$

Assim, na representação pretendida, o último algarismo (o das unidades) será o 1. A seguir a demonstração manda que se use a hipótese de indução. Isto equivale a repetir o raciocínio com o 595 e, se for o caso, fazer o mesmo com o quociente obtido. E assim por diante. Na prática pode-se proceder assim:

```
4761 |8
 76   595 |8
 41    35  74 |8
 (1)  (3) (2)  9 |8
              (1)(1)
```

Portanto:

$$4\,761 = (11231)_8$$

Exemplo 5: Dado o número $(2102)_3$, para passá-lo à base 5, por exemplo, pode-se primeiro encontrar sua representação decimal e depois proceder como no exemplo anterior.

$$(2102)_3 = 2 + 0 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^2 = 65$$

Então

$$\begin{array}{l|l} 65 & 5 \\ \hline 15 & 13 \;|\; 5 \\ \textcircled{0} & \textcircled{3}\textcircled{2} \end{array}$$

Logo: $(2102)_3 = (230)_5$

5.1 Operações

O procedimento usado em nosso sistema de numeração para efetuar adições e subtrações, ou seja, somando em coluna as unidades, depois as dezenas acrescidas de algum eventual transporte da coluna anterior e assim por diante é muito fácil de justificar. Examinemos, por exemplo, a adição 47 + 24:

$$\begin{array}{r} {}^{1} \\ + \; 47 \\ 24 \\ \hline 71 \end{array}$$

A soma das 7 unidades do primeiro número com as 4 do segundo é $11 = 1 + 1 \cdot 10$, uma unidade e uma dezena. Esta é então juntada às 4 dezenas de 47 e às duas de 24, obtendo-se as *7* dezenas da soma. Mas, embutidas nesse processo, estão as propriedades da adição em IN e, ainda, a propriedade distributiva. De fato:

$$47 + 24 = (4 \cdot 10 + 7) + (2 \cdot 10 + 4) =$$
$$= (4 \cdot 10 + 2 \cdot 10) + (7 + 4) = (4 \cdot 10 + 2 \cdot 10) + (1 \cdot 10 + 1) =$$
$$= (4 \cdot 10 + 2 \cdot 10 + 1 \cdot 10) + 1 = 7 \cdot 10 + 1$$

É claro que num sistema de base b posicional qualquer adição ou subtração pode ser efetuada da mesma maneira que o fazemos na base 10. Calculemos, por exemplo, $(4125)_6 + (1302)_6$:

$$\begin{array}{r} 1 \\ + \; (4125)_6 \\ (1302)_6 \\ \hline (5431)_6 \end{array}$$

Note-se que levamos em conta, na adição das unidades simples, que $5 + 2 = 7 = 1 \cdot 6 + 1 = (11)_6$ e por isso o resultado da coluna correspondente é 1, tendo sido transportado ainda, para a coluna seguinte, o algarismo 1.

Efetuemos agora a subtração $(2103)_4 - (1302)_4$:

$$\begin{array}{r} 1\,(11)_4 \\ - \; (\not{2}\;\not{1}\;0\;3)_4 \\ (1\;3\;0\;2)_4 \\ \hline (2\;0\;1)_4 \end{array}$$

Neste caso, como o número de unidades da terceira casa do minuendo é menor que o do subtraendo, foi preciso tomar emprestada uma unidade da casa seguinte. Como $(11)_4 = 1 \cdot 4^2 + 1 \cdot 4^3 = (1 + 1 \cdot 4) \cdot 4^2 = (3 + 2) \cdot 4^2 = 3 \cdot 4^2 + 2 \cdot 4^2$, o resultado na terceira coluna deve ser 2. Na prática o que se procura é o número que somado a 3 resulta $(11)_4 = 1 + 1 \cdot 4 = 5$

A multiplicação num sistema de numeração posicional de base b também pode ser efetuada segundo o procedimento usual da numeração decimal. E, assim como neste caso é preciso conhecer as tabuadas até a do 9, num sistema de base b tem que se partir de uma tábua de multiplicação (que pode estar na memória) para os números de 0 a b − 1. Calculemos por exemplo $(201)_3 \cdot (112)_3$. A tábua no caso é:

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

Assim, na base 3:

$$\begin{array}{r} 201 \\ 112 \\ \hline 1102 \\ 201+ \\ 201++ \\ \hline (100212)_3 \end{array}$$

uma vez que nesse caso $1 + 2 = 3 = 1 \cdot 3 + 0 = (10)_3$.

5.2 Critérios de divisibilidade

São bem conhecidos os critérios de divisibilidade da aritmética elementar. Mas, como justificá-los? De que maneira dependem eles de nosso sistema de numeração? Daremos resposta agora a essas perguntas em alguns casos. No capítulo III voltaremos ao assunto com uma ferramenta matemática mais potente para abordar a questão: a teoria das congruências.

Critério de divisibilidade por 2: Dado um número $n = a_0 + a_1 \cdot 10 + \ldots + a_r \cdot 10^r$, observando que toda potência 10^k ($k \geqslant 1$) é um número par, então:

$$n = a_0 + a_1(2q_1) + \ldots + a_r(2q_r) = a_0 + 2(a_1q_1 + \ldots + a_rq_r)$$

Ou seja

$$n = a_0 + 2q \ (q \in \mathbb{N})$$

Como $2q$ é divisível por 2, então n é divisível por 2 se, e somente se, a_0 é também divisível por 2. Ou seja, se e somente se $a_0 \in \{0, 2, 4, \ldots, 8\}$.

Critério de divisibilidade por 3: Primeiro observemos que o resto da divisão de 10^k por 3 é sempre 1, para todo $k \geqslant 0$. De fato, $10^0 = 1 = 3 \cdot 0 + 1$. Vamos supor $10^r = 3s + 1$, onde $r \geqslant 0$. Então $10^{r+1} = 10^r \cdot 10 = (3s + 1) \cdot (3 \cdot 3 + 1) = 3(9s) + 3s + 3 \cdot 3 + 1 = 3(9s + s + 3) + 1 = 3(10s + 3) + 1$.

Assim, para todo $n \in \mathbb{N}$:

$$\begin{aligned} n &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r = \\ &= a_0 + a_1(3q_1 + 1) + a_2(3q_2 + 1) + \ldots + a_r(3q_r + 1) = \\ &= (a_0 + a_1 + \ldots + a_r) + 3(a_1q_1 + a_2q_2 + \ldots + a_rq_r) \end{aligned}$$

Em resumo:

$$n = (a_0 + a_1 + \ldots + a_r) + 3q$$

Portanto n é divisível por 3 se, e somente se, $a_0 + a_1 + \ldots + a_r$ é divisível por 3 (propriedade $\mathbf{d_6}$).

Por exemplo: 1 761 é divisível por 3 já que $1 + 7 + 6 + 1 = 15$ o é. Já o número 226 não é divisível por 3 posto que $2 + 2 + 6 = 10$ não é múltiplo de 3.

A condição de divisibilidade de um número $n = a_0 + a_1 \cdot 10 + \ldots + a_r \cdot 10^r$ por 9 é semelhante à anterior: $9 \mid n \iff 9 \mid (a_0 + a_1 + \ldots + a_r)$. O motivo é que, também neste caso, $10^k = 9 \cdot s + 1$, para todo $k \in \mathbb{N}$.

Exemplo 6: Mostremos que um número $n = (a_ra_{r-1} \ldots a_1a_0)_{12}$ é divisível por 8 se, e somente se, o número $(a_1a_0)_{12}$ formado pelos dois últimos algarismos de n é divisível por 8.

Primeiro notemos que:

$$n = (a_1a_0)_{12} + a_2 \cdot 12^2 + a_3 \cdot 12^3 + \ldots + a_r \cdot 12^r$$

Mas, para $k \geqslant 2$, 12^k é divisível por 8. De fato, $12^2 = 144$ é múltiplo de 8. E se $12^s = 8 \cdot q_s$ ($s \geqslant 2$), então

$$12^{s+1} = 12^s \cdot 12 = (8q_s)12 = 8(12q_s)$$

Assim:

$$\begin{aligned} n &= (a_1a_0)_{12} + a_2(8q_2) + \ldots + a_r(8q_r) \\ &= (a_1a_2)_{12} + 8q \end{aligned}$$

Novamente a propriedade $\mathbf{d_6}$ garante nossa afirmação.

EXERCÍCIOS

32. (Fuvest-77) Calcule quantos múltiplos de três, de quatro algarismos distintos, podem ser formados com 2, 3, 4, 6 e 9.

Resolução: Com os cinco algarismos dados podem ser formados apenas três subconjuntos de quatro algarismos cuja soma dos elementos é divisível por 3: $\{2, 3, 4, 6\}$, $\{2, 3, 4, 9\}$ e $\{2, 4, 6, 9\}$. Cada um deles dá origem a 24 múltiplos de 3. Logo, a resposta é $3 \times 24 = 72$.

33. (UFMG-89) Seja $n = ab000$ um número não nulo, cujos cinco algarismos são a, b e três zeros. Se n é um quadrado perfeito e é divisível por 3, pode-se afirmar que $a + b$ é igual a:

a) 1 b) 6 c) 8 d) 9 e) 12

34. (Cesgranrio-88) Se cdu é o maior número de três algarismos divisível por 11, então a soma $c + d + u$ vale:

a) 22 b) 18 c) 20 d) 17 e) 16

Resolução: O maior número de três algarismos é 999, cuja divisão por 11 fornece resto 9. O número procurado é, então: $999 - 9 = 990$. Resposta: 18.

35. Quantos números naturais entre 1 e 1 000 são divisíveis por 9? E quantos, entre 250 e 25 000, são divisíveis por 11?

Sugestão (1ª parte): O primeiro desses números é 9 e o último 999. Conte o número de termos da P.A. em que o primeiro termo é 9, o último é 999 e a razão é 9.

36. (Cesgranrio-89) Se n é o número de múltiplos de 6 compreendidos entre 92 e 196, então n é:

a) 14 b) 15 c) 16 d) 17 e) 18

37. Se n e a são naturais não nulos, quantos números naturais entre 1 e n são divisíveis por a?

38. Prove que:

a) a soma de dois números pares é par e que a soma de dois números ímpares também é par.

b) o produto de dois números naturais é ímpar se, e somente se, ambos são ímpares.

39. Prove que o quadrado de um número natural a é par se, e somente se, a é par.

Resolução: Se a é par, então $a = 2t$, para algum $t \in \mathbb{N}$; daí $a^2 = (2t)^2 = 4t^2 = 2(2t^2)$ é par. Para a recíproca suponhamos que a fosse ímpar, digamos $a = 2r + 1$; então $a^2 = 4r^2 + 4r + 1 = 2(2r^2 + 2r) + 1$ é ímpar, o que não é possível.

40. Mostre que $a + b + a^2 + b^2$ é par, para quaisquer $a, b \in \mathbb{N}$.

41. Se a, b e c são números naturais não nulos, prove que: $a|b \iff ac|bc$.

42. Prove que: $(1 + 2 + \ldots + n)|3(1^2 + 2^2 + \ldots + n^2)$, para todo $n \geqslant 1$.

Sugestão: Lembrar que $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$ e usar o exercício 25-a.

43. Prove por indução que:

a) $7|(3^{2n+1} + 2^{n+2}), \forall n \geqslant 0$

b) $9|(10^n + 3 \cdot 4^{n+2} + 5), \forall n \geqslant 0$

c) $11|(2^{2n-1} \cdot 3^{n+2} + 1), \forall n \geqslant 1$

d) $17|(3^{4n+2} + 2 \cdot 4^{3n+1}), \forall n \geqslant 0$

Resolução de d): Seja $a(n) = 3^{4n+2} + 2 \cdot 4^{3n+1}$

$n = 0 : a(0) = 3^2 + 2 \cdot 4 = 17.$

Logo $17|a(0)$.

Seja $r \geqslant 0$ e suponhamos que $17|a(r)$, ou seja: $3^{4r+2} + 2 \cdot 4^{3r+1} = 17q$ para algum $q \in \mathbb{N}$.

Daí $2 \cdot 4^{3r+1} = 17q - 3^{4r+2}$.

$n = r + 1$: $a(r + 1) = 3^{4(r+1)+2} + 2 \cdot 4^{3(r+1)+1} =$
$= 3^{4r+6} + 2 \cdot 4^{3r+1} \cdot 4^3 = 3^{4r+6} + (17q - 3^{4r+2}) \cdot 64 =$
$= 17(64q) + 3^{4r+2} \cdot (3^4 - 64) = 17(64q + 3^{4r+2})$

44. Demonstre que de dois números pares consecutivos um é sempre divisível por 4.

45. (Unicamp-89) É possível encontrar dois números, ambos divisíveis por 7, tais que a divisão de um pelo outro deixe resto 39? Justifique a resposta.

46. Escreva o número 182 respectivamente nas bases 2, 8 e 12.

Obs.: No caso da base 12 use os algarismos indo-arábicos de 0 a 9 e as letras a e b para indicar, respectivamente, 10 e 11, se for preciso.

47. Efetue:

a) $(1034)_5 + (243)_5$

b) $(54302)_6 - (2134)_6$

c) $(1002)_4 \cdot (204)_4$

d) $(1025)_7 \cdot (1102)_7 + (21543)_7$

Resolução de d):

$(1025)_7$
$(1102)_7$
2053
1025
1025
$(1132553)_7$

$(1132553)_7$
$+ (21543)_7$
$(1154426)_7$

Notar que:

- $2 \cdot 5 = 10 = 1 \cdot 7 + 3 = (13)_7$
- $2 + 2 + 5 = 9 = 1 \cdot 7 + 2 = (12)_7$

onde levamos em conta que $1 + 5 + 5 = 11 = 1 \cdot 7 + 4 = (14)_7$.

48. Passe para o nosso sistema de numeração: $(10121)_3$, $(1042)_5$ e $(10\,ab)_{12}$, onde a representa "dez" e b "onze".

49. Construa a tábua de multiplicação referente à base 7.

50. Determine b em cada um dos seguintes casos:

a) $(104)_b = 8\,285$ b) $12\,551 = (30407)_b$.

51. Na divisão euclidiana de 802 por b o quociente é 14 e o resto r. Determine b e r.

Resolução: Por hipótese, $802 = b \cdot 14 + r$ $(r < b)$. Daí: $0 \leqslant 802 - 14 \cdot b = r < b$. Assim $14b \leqslant 802$ e $802 < 15b$. Os valores possíveis para esse sistema de desigualdades são $b = 54, 55, 56$ ou 57. Logo, respectivamente: $r = 46, 32, 18$ ou 4.

52. Mostre que para todo $n \in \mathbb{N}$ o número $\frac{n(n+1)}{2}$ está em $\mathbb{N}$ e que seu algarismo das unidades não pode ser 2, nem 4, nem 7 e nem 9.

Sugestão: Se o algarismo das unidades de $\frac{n(n+1)}{2}$ fosse um desses, o de $n(n+1)$ seria 4 ou 8. Mostre que isso não é possível.

53. Mostre que $(111)_b | (10101)_b$, para todo $b > 1$. Escreva o quociente da divisão em termos da base b.

54. Prove que: a) em todo sistema de numeração de base $b > 2$ o número $(121)_b$ é um quadrado perfeito; b) em todo sistema de numeração de base $b > 3$, o número $(1\,331)_b$ é um cubo perfeito.

Resolução de a): $(121)_b = 1 + 2 \cdot b + 1 \cdot b^2 = (1 + b)^2$

55. Determinar as condições sobre os naturais b e d, $b > 1$ e $d > 1$, a fim de que: $(14)_b = (22)_d$.

56. Seja n um número natural e $n = (a_r a_{r-1} \ldots a_2 a_1)_5$ sua representação na base 5. Prove que: $4 | n \iff 4 | (a_0 + a_1 + \ldots + a_n)$. Generalize este resultado para uma base qualquer $b > 2$.

Sugestão: Veja como foi justificado o critério de divisibilidade por 9 no nosso sistema de numeração.

57. (Fuvest-88)

$$\begin{array}{cccc} 1 & a & b & c \\ & \times & & 3 \\ \hline a & b & c & 4 \end{array}$$

Acima está representada uma multiplicação, onde os algarismos a, b e c são desconhecidos. Qual o valor da soma $a + b + c$?

a) 5
b) 8
c) 11
d) 14
e) 17

58. O produto de um número de três algarismos por 7 termina à direita em 638. Ache esse número.

59. a) Na divisão euclidiana de a por b, o quociente é 106 e o resto 304. Qual o maior número de que se pode aumentar dividendo e divisor sem que o quociente se altere?
b) E se $q = 356$ e $r = 4\,623$?

Resolução de a): Por hipótese $a = b \cdot 106 + 304$ $(304 < b)$. Acrescentando x ao dividendo e ao divisor, se 106 é o quociente da divisão de $a + x$ por $b + x$, então (segundo $4 \cdot 2$):

$(b + x) \cdot 106 \leqslant a + x < (b + x) \cdot 107$

Subtraindo $106b + x$ de cada um dos termos:

$$105x \leqslant 304 < b + 106x$$

A última desigualdade se verifica para todo x pois $304 < b$. Assim basta estudar $105x \leqslant 304$ que fornece as soluções $x = 0, 1$ ou 2. A resposta é então o número 2.

60. Se o algarismo das centenas do produto $a5 \cdot 164$ é 9, determine a (a representa um algarismo de nosso sistema de numeração).

61. Quantos números há num sistema de numeração de base b, formados de n algarismos? Qual o menor deles? (Escreva-o em função de b.)

6. Máximo divisor comum

DEFINIÇÃO 2 Sejam $a, b \in \mathbb{N}$. Um número $d \in \mathbb{N}$ se diz *máximo divisor comum* de a e b se: i $d | a$ e $d | b$; ii se c é um número natural tal que $c | a$ e $c | b$, então $c | d$.

Por exemplo, sejam $a = 6$ e $b = 8$. Indicando por D_x o conjunto dos divisores de $x \in \mathbb{N}$, então

$$D_6 = \{1, 2, 3, 6\} \quad \text{e} \quad D_8 = \{1, 2, 4, 8\}$$

do que segue:

$$D_6 \cap D_8 = \{1, 2\}$$

Observemos que: i $2 | 6$, $2 | 8$; ii se $c | 6$ e $c | 8$, então $c = 1$ ou $c = 2$ e portanto $c | 2$. Donde 2 é máximo divisor comum de 6 e 8.

Mostremos, de um modo geral, que não pode haver mais que um máximo divisor comum de a e b. De fato, se d e d' satisfazem a definição 2, então $d' | d$ (pois $d' | a$ e $d' | b$) e $d | d'$ (pois $d | a$, $d | b$ e d' é, por hipótese, máximo divisor comum de a e b), o que implica d = d'. Usaremos a notação d = mdc (a, b) para indicar o máximo divisor comum de a e b. Da definição decorre diretamente que mdc (a, b) = mdc (b, a).

Quanto à existência de máximo divisor comum, examinemos primeiro o caso a = 0 e b qualquer e mostremos que então b = mdc (0, b). De fato:

- $b | 0$ e $b | b$
- se $c | 0$ e $c | b$, obviamente $c | b$

Em particular mdc (0, 0) = 0. Note-se que neste último caso o máximo divisor comum não é o maior dos divisores comuns: como $1 | 0$, $2 | 0$, $3 | 0$, ... não há um maior divisor comum para 0 e 0.

Para a hipótese em que $a \neq 0$ e $b \neq 0$ precisaremos das duas proposições a seguir.

PROPOSIÇÃO 1 Se $a | b$, então mdc (a, b) = a.

Demonstração: De fato, $a | a$ e $a | b$ (hipótese). E se $c | a$ e $c | b$, é óbvio que $c | a$. ■

PROPOSIÇÃO 2 Se $a = bq + r$ e d = mdc (a, b), então d = mdc (b, r). E se d = mdc (b, r), então d = mdc (a, b).

Demonstração: Como d = mdc (a, b), então $d | a$ e $d | b$. Desta última relação resulta que $d | bq$. Logo $d | (a - bq)$, ou seja, $d | r$. Por outro lado, se $c | b$ e $c | r$, então $c | (bq + r)$ devido a $\mathbf{d_4}$, item 4.1; como $bq + r = a$, então $c | a$ e $c | b$, o que implica $c | d$, já que d = mdc (a, b).

A segunda afirmação se prova de maneira análoga. ■

Retomemos agora a questão da existência de máximo divisor comum. Para provar a existência aplicaremos, sucessivamente, a partir de a e b, o algoritmo da divisão da seguinte maneira:

$$a = bq_1 + r_1 \ (r_1 < b)$$
$$b = r_1 q_2 + r_2 (r_2 < r_1)$$
$$r_1 = r_2 q_3 + r_3 \ (r_3 < r_2)$$
$$\vdots$$

É claro que, se acontecer de r_1 ser nulo, então a proposição 1 nos garante que b = mdc (a, b) e o processo termina na primeira etapa. Mas, de qualquer maneira, na seqüência $b > r_1 > r_2 > r_3 > \dots$ para algum índice n deverá ocorrer

$r_{n+1} = 0$. De fato, se todos os r_i fossem não nulos, então $\{b, r_1, r_2, \dots\}$ não teria mínimo, o que não é possível. Assim, para algum n:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$
$$r_{n-1} = r_n \cdot q_{n+1}$$

Como conseqüência das proposições anteriores, obtém-se então o seguinte:

$$r_n = \text{mdc}\ (r_{n-1}, r_n) = \text{mdc}\ (r_{n-2}, r_{n-1}) = \dots = \text{mdc}\ (b, r_1) = \text{mdc}\ (a, b)$$

Ou seja:

$$r_n = \text{mdc}\ (a, b)$$

Essa demonstração obviamente é construtiva e o dispositivo prático que se costuma empregar para aplicá-la é conhecido como *processo das divisões sucessivas*.

Exemplo 7: Achemos, por esse processo, mdc (41, 12).

$$41 = 12 \cdot 3 + 5$$
$$12 = 5 \cdot 2 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

Logo, 1 = mdc (41, 12). Usualmente procede-se assim:

	3	2	2	2
41	12	5	2	①
5	2	1	0	

Recomendamos comparar esse quadro com a sucessão anterior de igualdades.

DEFINIÇÃO 3 Dois números naturais a e b se dizem *primos entre si* se mdc (a, b) = 1. Neste caso diz-se também que a é *primo com* b ou vice-versa.

Exemplo 8: Dois números *consecutivos* a e a + 1 são sempre primos entre si.

De fato, é claro que $1 | a$ e $1 | (a + 1)$. Agora, se $c | a$ e $c | (a + 1)$, então $c | [(a + 1) - a]$, ou seja, $c | 1$.

PROPOSIÇÃO 3 Se d = mdc (a, b), então mdc (sa, sb) = sd, para todo $s \in \mathbb{N}$.

Demonstração: Multipliquemos por s cada uma das igualdades obtidas pelo algoritmo da divisão no processo das divisões sucessivas que leva a d, a partir de a e b:

$$sa = (sb)q_1 + sr_1$$
$$sb = (sr_1)q_2 + sr_2$$
$$\vdots$$
$$sr_{n-2} = (sr_{n-1})q_n + sr_n$$
$$sr_{n-1} = (sr_n)q_{n+1}$$

As proposições 1 e 2 nos garantem então que:

$$sd = sr_n = \text{mdc}(sr_{n-1}, sr_n) = \ldots = \text{mdc}(sb, sr_1) = \text{mdc}(sa, sb). \quad \blacksquare$$

COROLÁRIO 1 Se $a, b \in \mathbb{N}^*$ e $d = \text{mdc}(a, b)$, então $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Ou seja: $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si:

Demonstração: Como

$d = \text{mdc}(a, b) = \text{mdc}\left(d\,\frac{a}{d}, d\,\frac{b}{d}\right) = d\,\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right)$ e $d \neq 0$, então:

$$\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \quad \blacksquare$$

COROLÁRIO 2 Se $a|bc$ e $\text{mdc}(a, b) = 1$, então $a|c$.

Demonstração: Da hipótese $\text{mdc}(a, b) = 1$ decorre, levando em conta a proposição 3, que

$$\text{mdc}(ac, bc) = c$$

Como $a|bc$ por hipótese e obviamente $a|ac$, então $a|\text{mdc}(ac, bc)$. Ou seja $a|c$. ■

COROLÁRIO 3 Se a e b são divisores de $c \neq 0$ e $\text{mdc}(a, b) = 1$, então $ab|c$.

Demonstração: De $\text{mdc}(a, b) = 1$ decorre, em virtude da proposição 3, que $\text{mdc}(ac, bc) = c$. Mas $ab|ac$, pois $b|c$ e $ab|bc$ já que $a|c$. Logo ab divide $\text{mdc}(ac, bc)$, isto é, $ab|c$. ■

Por exemplo, para que um número seja divisível por 6 é necessário e suficiente que seja divisível por 2 e por 3 já que mdc (2, 3) = 1.

Generalização: A definição de máximo divisor comum pode ser estendida de maneira óbvia para três ou mais números. Para o cálculo do máximo divisor comum de três números, por exemplo, pode-se lançar mão do seguinte resultado:

$$\text{mdc}(a, b, c) = \text{mdc}(\text{mdc}(a, b), c) = \text{mdc}(a, \text{mdc}(b, c))$$

Provemos a primeira dessas igualdades. Seja $d = \text{mdc}(a, b, c)$. Então $d|a$, $d|b$ e $d|c$. Das duas primeiras dessas relações segue que $d|\text{mdc}(a, b)$. Assim: $d|\text{mdc}(a, b)$ e $d|c$. Seja, agora, k um divisor de $d_1 = \text{mdc}(a, b)$ e de c. Como $d_1|a$ e $d_1|b$, pela transitividade chega-se a que $k|a$, $k|b$ e $k|c$. Logo $k|d$ pois $d = \text{mdc}(a, b, c)$. A demonstração fica completa considerando-se a unicidade do máximo divisor comum.

Achemos, por exemplo, mdc (6, 8, 20).

	1	3
8	6	(2)
2	0	

mdc (6, 8) = 2

Como, ademais, mdc (2, 20) = 2, pois $2|20$, então:

$$\text{mdc}(6, 8, 20) = 2.$$

7. Mínimo múltiplo comum

DEFINIÇÃO 4 Um número m se diz *mínimo múltiplo comum* de $a, b \in \mathbb{N}$ se: **i** $a|m$ e $b|m$ (m é múltiplo de a e de b); **ii** $a|m'$ e $b|m' \Rightarrow m|m'$ (todo múltiplo de a e b é também múltiplo de m).

Se m e m_1 satisfazem essa definição, então $m|m_1$ (pois m_1 é múltiplo de a e b) e $m_1|m$ (já que m é múltiplo de a e b e m_1 é mínimo múltiplo comum de a e b). Logo $m = m_1$. Ou seja, dois números a e b não podem ter mais que um mínimo múltiplo comum. Se m é mínimo múltiplo comum de a e b, usaremos a notação $m = \text{mmc}(a, b)$. Da definição decorre diretamente que $\text{mmc}(a, b) = \text{mmc}(b, a)$.

Quanto à existência de mínimo múltiplo comum, consideremos inicialmente o caso a = 0 e b qualquer. Mostremos que mmc (0, b) = 0. De fato:

- $0|0$ e $b|0$ (pois $0 = b \cdot 0$)
- $0|m'$ e $b|m' \Rightarrow 0|m'$

Para os demais casos a garantia de existência é dada pela

PROPOSIÇÃO 4 Para quaisquer a, b $\in$ IN*, se d = mdc (a, b), então $m = \frac{ab}{d}$ é o mínimo múltiplo comum de a e b.

Demonstração: Notemos primeiro que como $d|(ab)$ (pois $d|a$ e $d|b$), então $m \in$ IN.

i Como, evidentemente,

$$a\frac{b}{d} = \frac{ab}{d} = m$$

então $a|m$. Analogamente se mostra que $b|m$.

ii Seja m' um múltiplo de a e de b e suponhamos m' = ar e m' = bs. Então ar = bs e portanto:

$$\frac{a}{d}r = \frac{b}{d}s$$

Daí segue que $\frac{a}{d}$ divide $\frac{b}{d}s$ e, como mdc $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ então $\frac{a}{d}|s$ (corolário 2 — proposição 3). Assim

$$s = \frac{a}{d}t$$

para algum t $\in$ IN e como m' = bs, obtemos

$$m' = b\frac{a}{d}t = \frac{ab}{d}t = mt$$

ou seja: $m|m'$. ■

COROLÁRIO Se a e b são primos entre si, então mmc (a, b) = ab.

De fato, como d = mdc (a, b) = 1, então mmc (a, b) = $\frac{ab}{1}$ = ab. ■

Nota: Sejam a, b $\in$ IN*. Pelo que vimos $\frac{ab}{d} = m \in M_a \cap M_b$. Mas $0 \in M_a \cap M_b$ e como $m > 0$, então m não é o menor dos múltiplos comuns de a e b. Na verdade, neste caso m = mmc (a, b) é o menor dos múltiplos comuns não nulos de a e b.

Exemplo 9: Vamos usar a proposição anterior para achar mmc (20, 8). Como

	2	2
20	8	(4)
4	0	

mdc (20, 8) = 4

então mmc (20, 8) = $\frac{20 \cdot 8}{4}$ = 40.

PROPOSIÇÃO 5 Se m = mmc (a, b), então mmc (sa, sb) = sm, para qualquer s $\in$ IN.

Demonstração: Quando a = 0 ou b = 0, então m = 0 e sa = 0 ou sb = 0; daí mmc (sa, sb) = 0 = sm. Se s = 0, ficamos com mmc (0, 0) = 0, que também é verdadeira. Suponhamos por fim a, b e s não nulos; levando em conta as duas proposições anteriores:

$$\text{mmc}(sa, sb) = \frac{sa\,sb}{\text{mdc}(sa, sb)} = \frac{s^2 ab}{s\,\text{mdc}(a, b)} = s\frac{ab}{\text{mdc}(a, b)} =$$
$$= s\,\text{mmc}(a, b).$$ ■

Generalização: A extensão do conceito de mínimo múltiplo comum em IN para 3 ou mais números se faz naturalmente. No caso de 3 números, por exemplo, o cálculo pode ser feito com base na seguinte propriedade cuja demonstração omitimos (recomendamos como exercício):

mmc (a, b, c) = mmc (a, mmc (b, c)) = mmc (mmc (a, b), c)

Por exemplo:

mmc (3, 5, 20) = mmc (mmc (3, 5), 20) = mmc (15, 20) = 60

EXERCÍCIOS

62. Ache:

a) mdc (648, 140) e mmc (648, 140)

b) mdc (60, 132, 64) e mmc (60, 132, 64)

63. O máximo divisor comum de dois números é 48 e o maior deles é 384. Ache o outro número.

Resolução: Seja b o número procurado. Como $\frac{384}{48} = 8$, então $\frac{b}{48} < 8$ e mdc $\left(8, \frac{b}{48}\right) = 1$ (corolário 1, propos. 3). Assim os valores possíveis de $\frac{b}{48}$ são 1, 3, 5 ou 7 e portanto b = 48, 144, 240 ou 336.

64. O máximo divisor comum de dois números é 20. Para se chegar a esse resultado pelo processo das divisões sucessivas, os quocientes encontrados foram, pela ordem, 2, 1, 3 e 2. Ache os números.

65. Encontre dois números naturais cuja soma é s = 304 e cujo mdc é 16.

Resolução: Se a e b são os números, então 304 : 16 = a : 16 + b : 16 = = 19. Como mdc (a : 16, b : 16) = 1, então a : 16 e b : 16 podem ser iguais a: 1 e 18, 2 e 17, 3 e 16, 4 e 15, 5 e 14, 6 e 13, 7 e 12, 8 e 11, 9 e 10 (as demais possibilidades nada acrescentam à resposta). Logo as soluções são: 16 e 288, 32 e 272, ..., 144 e 160 (9 ao todo).

66. Ache dois números cujo produto é 4 800 e seu mdc é 20.

67. Prove que mdc (n, 2n + 1) = 1, para todo $n \in \mathbb{N}$.

68. Demonstre que dois números ímpares consecutivos são primos entre si.

Resolução: Se r é um divisor comum aos dois números, então r divide 2, que é a diferença entre o maior e o menor. Logo r = 1, pois r não pode ser par, uma vez que é divisor de números ímpares.

69. Se n e k são números naturais não nulos e mdc (n, n + k) = 1, prove que mdc (n, k) = 1.

70. Se $a, b \in \mathbb{N}$, prove que mdc (a, ab + 1) = mdc (b, ab + 1) = 1.

71. Prove que mdc (a + bc, b) = mdc (a, b), para quaisquer $a, b, c \in \mathbb{N}$.

Resolução: Seja d = mdc (a, b) e provemos que d = mdc (a + bc, b). Como d|a e d|b, então d divide a + bc. Seja r um divisor de a + bc e de b; de r|b resulta que r|bc; então r|(a + bc) e r|(bc) e portanto r|a; dividindo a e b, então r|d = mdc (a, b).

72. (Magistério 1º e 2º graus — SP-86) Sendo q um número natural diferente de zero e $A_q = \{n \in \mathbb{N}$: n é múltiplo de q$\}$, a frase verdadeira é:

a) $A_p \cup A_q = A_{pq}$

b) se $p \neq q$, então $A_p \cap A_q = \emptyset$

c) se $r \in A_q$, $r \neq 0$, então $A_r \subset A_q$

d) existe $q \in \mathbb{N}$, $q > 0$, tal que $A_q = \emptyset$

e) $A_p \cap A_q = A_r$, onde r = mdc (p, q)

73. Se a e b são números naturais primos entre si, prove que mdc (a + b, $a^2 + ab + b^2$) = 1.

74. Se a, b e c são números naturais e b|c, prove que mdc (a, b) = mdc (a + c, b).

75. Se a, b e c são números naturais não nulos, prove que mdc (a, b) é um divisor de mdc (a, bc).

76. Se mdc (a, c) = 1, prove que mdc (a, bc) = mdc (a, b), para todo $b \in \mathbb{N}$.

Resolução: Da hipótese decorre que mdc (ab,bc) = b. Como porém mdc (ab, bc) é divisível por mdc (a, bc), devido ao exercício 75, então mdc (a, bc)|b; observando que mdc (a, bc)|a, conclui-se então que mdc (a, bc)|mdc (a, b). Levando em conta que mdc (a, b)|mdc (a, bc), ainda devido ao exercício 75, fica estabelecida a igualdade do enunciado.

77. Se mdc (a, 4) = 2 e mdc (b, 4) = 2, prove que mdc (a + b, 4) = 4.

78. Sejam a, b e c três números ímpares arbitrários. Prove que:

$$\text{mdc}\,(a, b, c) = \text{mdc}\left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right)$$

79. Prove que o produto de três números naturais consecutivos é divisível por 6.

Sugestão: Se 2|a e 3|a, então 6|a, pois mdc (2, 3) = 1.

80. (Unicamp-88) Os planetas Júpiter, Saturno e Urano têm períodos de revolução em torno do Sol de aproximadamente 12, 30 e 84 anos, respectivamente. Quanto tempo decorrerá, depois de uma observação, para que eles voltem a ocupar simultaneamente as mesmas posições em que se encontravam no momento da observação?

81. Determine todos os números de três algarismos divisíveis por 8, 11 e 12.

82. Determine o menor número natural que dividido por 12, 20 e 38 dá o mesmo resto 10. 1150

83. (Cesgranrio-88) Seja N um inteiro tal que $200 < N < 300$; seja igual a 2 o resto da divisão de N por 3, por 5 ou por 8. Então a soma dos algarismos de N é:

a) 5 b) 7 c) 8 d) 10 e) 12

84. Ache dois números naturais conhecendo seu mdc 12 e seu mmc 240.

Resolução: Sejam a e b os números. Então $12 \cdot 240 = ab$, em virtude da proposição 4. Daí $\frac{a}{12} \cdot \frac{b}{12} = 20$, e como mdc $\left(\frac{a}{12}, \frac{b}{12}\right) = 1$, então $\frac{a}{12} = 1$ e $\frac{b}{12} = 20$, ou $\frac{a}{12} = 4$ e $\frac{b}{12} = 5$. As possíveis soluções são, portanto: 12 e 240 ou 48 e 60.

85. Ache dois números naturais cuja soma é 120 e cujo mmc é 144.

86. Seja m o mínimo múltiplo comum de dois números naturais não nulos a e b. Prove que:

$$\text{mdc}\left(\frac{m}{a}, \frac{m}{b}\right) = 1$$

8. Números primos

DEFINIÇÃO 5 Um número $p \in \mathbb{N}$ se diz *primo* se i $p \neq 0$ e $p \neq 1$; ii Os únicos divisores de p são 1 e p. Um número $a \in \mathbb{N}$, $a \neq 0$ e $a \neq 1$, é chamado *composto* se a não é primo. Assim, um número composto sempre pode ser fatorado num produto $a = bc$, onde $b \neq 1$ e $c \neq 1$.

Observemos que 0 e 1 não são primos nem compostos.

Por exemplo: o número 2 é primo pois, se $a|2$, então $0 < a \leqslant 2$ e portanto $a = 1$ ou $a = 2$. O número 2 é o único primo par pois, se $a > 2$ é par, então $a = 2q$ onde $q > 1$ e portanto 1, 2 e q são divisores de a, distintos entre si.

PROPOSIÇÃO 6 Se p é primo e $p|ab$, então $p|a$ ou $p|b$. (Por indução: se p é primo e $p|(a_1 a_2 \ldots a_r)$, $r \geqslant 1$, então p divide algum dos a_i.)

Demonstração: Suponhamos $a \neq 0$ e $b \neq 0$ (o caso $a = 0$ ou $b = 0$ é imediato). Admitamos que $p \nmid a$ e provemos que mdc $(a, p) = 1$. De fato, se $c|a$ e $c|p$, então $c = 1$ ou $c = p$ (pois p é primo); como porém $p \nmid a$, então $c = 1$. O corolário 2 da proposição 3 nos assegura então que $p|b$. ■

PROPOSIÇÃO 7 Seja $a \in \mathbb{N}$, $a \neq 0$ e $a \neq 1$. Então o mínimo de $S = \{x \in \mathbb{N}: x > 1 \text{ e } x|a\}$ é um número primo.

Demonstração: $S \neq \emptyset$ pois $a \in S$. Seja p o mínimo de S. Se p não fosse primo, como $p \neq 0$ e $p \neq 1$, então existiriam $b, c \in \mathbb{N}$, $b \neq 1$ e $c \neq 1$, de modo que $p = bc$ e daí $b < p$. Como b, por ser um divisor de p, também divide a, então b é um divisor de a menor que p, além de diferente de 1. Este absurdo mostra que p é primo. ■

TEOREMA 3 (*teorema fundamental da aritmética*): Para todo número natural $a > 1$ existem números primos $p_1, p_2, \ldots, p_r$ ($r \geqslant 1$), de maneira que $a = p_1 \cdot p_2 \ldots p_r$. Além disso, se também $a = q_1 \cdot q_2 \ldots q_s$ ($s \geqslant 1$), onde os q_i são igualmente primos, então $r = s$ e cada p_i é igual a algum dos q_j.

Demonstração:

a) Usaremos o segundo princípio de indução. Se $a = 2$, como 2 é primo, a afirmação de existência é trivialmente verdadeira. Suponhamos $a > 2$ e o teorema válido, em sua primeira afirmação, para todo b, $2 \leqslant b < a$. A proposição anterior nos garante que a admite um divisor primo p_1 : $a = p_1 \cdot a_1$ ($a_1 \in \mathbb{N}^*$). Se $a_1 = 1$ ou a_1 é primo, a demonstração se encerra. Caso contrário, visto que então $2 \leqslant a_1 < a$, a hipótese de indução nos assegura que há $r - 1$ primos $p_2, \ldots, p_r$ ($r - 1 \geqslant 1$) de modo que $a_1 = p_2 \cdot p_3 \ldots p_r$. Donde $a = p_1 \cdot p_2 \ldots p_r$.

b) Em rigor teríamos que raciocinar por indução. Mas não seremos formais nesta parte.
Se $p_1 \cdot p_2 \ldots p_r = q_1 \cdot q_2 \ldots q_s$, conforme o enunciado, então p_1 divide o segundo membro e portanto (proposição 6) divide um de seus fatores, digamos q_1. Sendo apenas 1 e q_1 os divisores de q_1 e sendo $p_1 \neq 1$, então $p_1 = q_1$. Cancelando p_1 com q_1 na igualdade inicial, obtemos $p_2 \cdot p_3 \ldots p_r = q_2 \cdot q_3 \ldots q_s$. Repetindo essa argumentação o quanto for necessário, chegaremos à unicidade conforme o enunciado. É claro que não poderá ocorrer ao fim algo como $1 = q_{r+1} \ldots q_s$, pois isto implicaria $q_s|1$, o que não é possível pois q_s é primo. ■

Exemplo 10: O processo prático elementar usado para decompor um número em fatores primos é baseado nos resultados anteriores. Por exemplo, se $a = 84$, faz-se:

84	2
42	2
21	3
7	7
1	

$$84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3 \cdot 7$$

A explicação é a seguinte: o menor divisor de 84, excluído o 1, é primo (no caso o 2); o menor divisor de 42, excluído o 1, também é primo e é igualmente divisor de 84 (no caso o 2). É claro, então, que esse raciocínio leva à decomposição de 84 em fatores primos conforme o teorema 3.

Exemplo 11: Do que vimos decorre que todo número primo ou composto admite um divisor primo. Isto é muito útil às vezes, como para resolver o seguinte exercício(*): "Prove que se a e b são primos entre si, então ab e a + b também são primos entre si."

Suponhamos mdc (ab, a + b) = d > 1. Então d admite um divisor primo p que, por sua vez, também é divisor de ab e a + b. Ora, se $p|ab$, então $p|a$ ou $p|b$. Supondo $p|a$, como $p|(a+b)$, então $p|b$ pois $b = (a+b) - a$. Logo, $p|$mdc (a, b), o que é absurdo pois mdc (a, b) = 1.

8.1 Sobre a decomposição em fatores primos

I Na decomposição $a = p_1 p_2 \dots p_r$, conforme o teorema 3, é claro que nem sempre todos os fatores são diferentes entre si. A reunião de possíveis fatores iguais leva à expressão

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

onde $1 \leqslant s \leqslant r$, $p_i \neq p_j$ sempre que $i \neq j$ e $\alpha_i \geqslant 1$ $(i = 1, 2, \dots, s)$. Se, além disso, impusermos $p_1 < p_2 < \dots < p_s$, teremos a chamada *decomposição canônica* de a.

II Pode ser conveniente às vezes que, ao lidar com dois ou mais números maiores que 1, estejam eles escritos como potências dos mesmos primos. Isso é possível, obviamente, desde que se utilizem expoentes nulos, como no exemplo a seguir:

$$120 = 2^3 \cdot 3 \cdot 5 \cdot 7^0 \qquad \text{e} \qquad 350 = 2 \cdot 3^0 \cdot 5^2 \cdot 7$$

III De **I** e **II** decorre, considerando ainda o teorema fundamental da aritmética, o seguinte critério:

Dado $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s}$, conforme **I** ou **II**, então um número b é divisor de a se, e somente se, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s}$, onde $0 \leqslant \beta_i \leqslant \alpha_i$ $(i = 1, 2, \dots, s)$. De fato, se $b|a$, o teorema fundamental da aritmética obriga a que não haja fatores primos de b que não sejam fatores primos de a. Mas nem todos os fatores primos de a precisam estar na decomposição de b em primos. Daí os possíveis expoentes nulos em fatores de b, mesmo que não os haja em a. Quanto à recíproca, tomando $c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \dots p_s^{\gamma_s}$, onde $\gamma_i = \alpha_i - \beta_i$ $(i = 1, 2, \dots, s)$, então $c \in \mathbb{N}$ e $c \cdot b = a$. Logo $b|a$.

(*) Concurso de Ingresso ao Magistério de Primeiro e Segundo Grau do Estado de São Paulo — 1986.

Exemplo 12: É possível provar, usando as observações anteriores, que, para todo $k \geqslant 1$:

$$a^k | b^k \Rightarrow a | b$$

Justificaremos esse fato para k = 2. Seja $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s}$, conforme **I**. Então $b^2 = p_1^{2\beta_1} \cdot p_2^{2\beta_2} \dots p_s^{2\beta_s}$. Como $a|a^2$ e $a^2|b^2$ (hipótese), então não figuram em a fatores primos outros que $p_1, \dots, p_s$. Ou seja: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s}$, onde $\alpha_i \geqslant 0$ $(i = 1, 2, \dots, s)$. Logo

$$a^2 = p_1^{2\alpha_1} \cdot p_2^{2\alpha_2} \dots p_s^{2\alpha_s}$$

e $0 \leqslant 2\alpha_i \leqslant 2\beta_i$ $(1 \leqslant i \leqslant s)$, em virtude da hipótese de que $a^2|b^2$. Mas então $0 \leqslant \alpha_i \leqslant \beta_i$ para todo índice i e portanto $a|b$.

Exemplo 13: **Fórmula do número de divisores**

Para todo $a \in \mathbb{N}^*$, indica-se por $\tau(a)$ o número de divisores de a. Por exemplo: $\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 2$, $\tau(4) = 3$ (os divisores de 4 são 1, 2, 4 — três no total). Se p é primo, então $\tau(p) = 2$. Note-se que τ é uma função numérica definida em $\mathbb{N}^*$.

Vamos determinar uma fórmula para $\tau(a)$, sempre que $a > 1$. Supondo

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s} \; (\alpha_1, \dots, \alpha_s \geqslant 1)$$

conforme I, então, levando em conta que

$$b|a \iff b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s} \; (0 \leqslant \beta_i \leqslant \alpha_i;\ i = 1, 2, \dots, s)$$

a questão pode ser encarada sob o ponto de vista da Combinatória: como cada β_i pode assumir, independentemente, os $\alpha_i + 1$ valores $0, 1, 2, \dots, \alpha_i$, então:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)$$

Por exemplo, quantos divisores tem o número 48? Como $48 = 2^4 \cdot 3$, então

$$\tau(48) = (4 + 1) \cdot (1 + 1) = 10$$

IV Considerando o tipo de decomposição fornecida por **II**, pode-se provar que para quaisquer números não nulos a e b, se

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s} \quad \text{e} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s}$$

e se $\gamma_i = \min\{\alpha_i, \beta_i\}$, então

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \dots p_s^{\gamma_s}$$

é o máximo divisor comum de a e b.

De fato, pelo que já vimos em **III**, $d|a$ e $d|b$. Agora, se $c \in \mathbb{N}$ é um divisor de a e b, então (ainda devido a **III**)

$$c = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \dots p_s^{\lambda_s}$$

onde $0 \leqslant \lambda_i \leqslant \alpha_i$ e $0 \leqslant \lambda_i \leqslant \beta_i$ $(i = 1, 2, \dots, s)$. Mas então, para cada um desses índices, i:

$$0 \leqslant \lambda_i \leqslant \min\{\alpha_i, \beta_i\} = \gamma_i$$

pois $\min\{\alpha_i, \beta_i\} = \alpha_i$ ou $\min\{\alpha_i, \beta_i\} = \beta_i$. Donde $c|d$.

Por exemplo, se $a = 48 = 2^4 \cdot 3$ e $b = 50 = 2 \cdot 5^2$, como $48 = 2^4 \cdot 3 \cdot 5^0$ e $50 = 2 \cdot 3^0 \cdot 5^2$, então:

$$\text{mdc}\,(48, 50) = 2 \cdot 3^0 \cdot 5^0 = 2$$

A regra elementar segundo a qual o máximo divisor comum de dois números naturais não nulos é o produto dos fatores primos comuns, cada um com o menor expoente, é apenas uma versão do resultado deste item.

V Se a e b são naturais não nulos que se fatoram, consoante **II**, como

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s} \quad \text{e} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s}$$

e se $\delta_i = \max\{\alpha_i, \beta_i\}$ $(1 \leqslant i \leqslant s)$, então

$$m = p_1^{\delta_1} \cdot p_2^{\delta_2} \dots p_s^{\delta_s}$$

é o mínimo múltiplo comum de a e b.

Que é múltiplo decorre diretamente de **III**. Além disso, se $m' = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \dots p_s^{\lambda_s}$ é múltiplo de a e de b, então $\lambda_i \geqslant \alpha_i \geqslant 0$ e $\lambda_i \geqslant \beta_i \geqslant 0$ $(i = 1, 2, \dots; s)$. Logo $\lambda_i \geqslant \max\{\alpha_i, \beta_i\} = \delta_i$ $(i \leqslant i \leqslant s)$ e então $m|m'$.

Por exemplo:

$$\text{mmc}\,(48, 50) = 2^4 \cdot 3 \cdot 5^2 = 1\,200$$

8.2 *Números primos: um conjunto infinito*

Há 168 números primos entre 1 e 1 000, 135 entre 1 000 e 2 000 e 127 entre 2 000 e 3 000. Os dados de que dispomos hoje a respeito vão muito além

mas, mesmo com os computadores eletrônicos, há limitações para pesquisas nesse sentido. Contudo, já nos *elementos*, de Euclides, apareceu uma demonstração, que será reproduzida aqui, garantindo que o conjunto dos números primos é infinito.

Um conjunto $A \neq \varnothing$ se diz *infinito* se, para todo $n \geqslant 1$ $(n \in \mathbb{N})$, não é possível estabelecer uma correspondência biunívoca entre $\{1, 2, \dots, n\}$ e A.

Mostraremos primeiro que há em $\mathbb{N}$ intervalos arbitrariamente grandes sem números primos.

PROPOSIÇÃO 8 Para todo $n \in \mathbb{N}^*$ há uma seqüência de n números naturais consecutivos na qual nenhum elemento é primo.

Demonstração: Seja $n! = 1 \cdot 2 \cdot 3 \dots n$ e consideremos a seqüência $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$ que, é claro, tem n números naturais. Mostremos que nenhum deles é primo. Para todo k, $2 \leqslant k \leqslant n+1$, como

$$(n+1)! = (n+1)n \dots k \dots 2 \cdot 1$$

então $k|[(n+1)! + k]$ pois divide cada parcela dessa soma. Como $2 \leqslant k < (n+1)! + k$, então efetivamente nenhum dos números $(n+1)! + k$ é primo. ■

Por exemplo, se $n = 5$, então na seqüência

$6! + 2 = 722$, $6! + 3 = 723$, $6! + 4 = 724$, $6! + 5 = 725$ e $6! + 6 = 726$

nenhum número é primo.

PROPOSIÇÃO 9 (Euclides) O conjunto dos números primos é infinito.

Demonstração (por redução ao absurdo): Vamos supor que fosse finito. Então existiria um número natural $r > 1$ tal que seria possível indicar todos os números primos da seguinte maneira: $p_1, p_2, \dots, p_r$. Consideremos o número natural

$$n = p_1 \cdot p_2 \dots p_r + 1$$

Como, pela proposição 7, n admite um divisor primo p e $p_1, p_2, \dots, p_r$ são, por hipótese, todos os números primos, então $p = p_i$ para algum i $(1 \leqslant i \leqslant r)$. Assim, $p|n$ e $p|(p_1 p_2 \dots p_i \dots p_r)$, o que implica que $p|1$, pois $1 = n - p_1 p_2 \dots p_r$. Absurdo. Então, realmente, há uma infinidade de primos. ■

8.3 O crivo de Eratóstenes

Neste item estabeleceremos um critério para determinar se um número é primo ou não e um processo (chamado *crivo de Eratóstenes*) para encontrar todos os primos de 1 até um certo $n \in \mathbb{N}^*$. A razão do nome dado ao processo é que, para aplicá-lo, parte-se de um quadro formado pelos números naturais de 1 a n do qual se vão eliminando, por etapas, os elementos que não são primos.

Eratóstenes de Cirene (aprox. 280-192 a.C.) foi um sábio de atividades várias: além de matemático foi astrônomo, geógrafo e filólogo. Quando tinha cerca de 40 anos de idade passou a dirigir a célebre biblioteca de Alexandria. É mais conhecido, provavelmente, pela medição que fez, bastante boa para a época, da circunferência da Terra.

PROPOSIÇÃO 10 Se $n > 1$ é um número composto, então há um número primo p tal que:

$$p|n \text{ e } p^2 \leqslant n \ (\iff p \leqslant \sqrt{n})$$

Demonstração: Por hipótese, n pode ser decomposto da seguinte maneira:

$$n = ab \ (2 \leqslant a \leqslant b < n)$$

Logo, $n = ab \geqslant a^2$. Seja p um divisor primo de a. Então $p^2|a^2$ e portanto $p^2 \leqslant a^2$. Donde $p^2 \leqslant n$, o que pode ser traduzido por $p \leqslant \sqrt{n}$. ■

Conseqüência: Se um número $n > 1$ não é divisível por nenhum dos primos $p \leqslant \sqrt{n}$, então n é primo.

De fato, se fosse composto, pela proposição 10 admitiria um divisor primo menor ou igual a $\sqrt{n}$.

Exemplo 14: O número 271 é primo ou composto? Primeiro observemos que $16 \leqslant \sqrt{271} < 17$. Os primos que não superam 16 são: 2, 3, 5, 7, 11 e 13. Mas nenhum deles é divisor de 271. Logo, este número é primo.

Explicaremos agora o procedimento do crivo de Eratóstenes. Inicialmente faz-se uma tabela com os números de 2 a n. No quadro obtido devem ser cancelados todos os múltiplos de 2, exceto o 2, todos os múltiplos de 3, exceto o 3, os de 5, exceto o 5, e assim por diante. É claro que dessa forma não sobrarão senão números primos sem ser atingidos. Mas é importante saber, nesse processo, em que primo p parar, por serem desnecessárias as etapas seguintes. A resposta é: $2 \leqslant p \leqslant \sqrt{n}$.

De fato, seja a um número natural, $2 < a \leqslant n$. Se a é composto, então existe um primo p tal que $p|a$ e $p \leqslant \sqrt{a}$. Daí se conclui que $p \leqslant \sqrt{n}$. Logo, o número a será efetivamente cancelado quando se aplica o processo para os primos $p \leqslant \sqrt{n}$.

Exemplo 15: Achemos todos os números primos $\leqslant 50$. Como $7 < \sqrt{50} < 11$, então basta trabalhar com os primos 2, 3, 5 e 7. Assim

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

Observe que o 49 foi cancelado na última etapa necessária do processo.

8.4 Os números de Fermat

Deixaremos para demonstrar no capítulo seguinte (por ser mais cômodo naquela altura) que se $p = 2^m + 1$ ($m \in \mathbb{N}^*$) é primo, então m é uma potência de 2 (exercício 249).

Talvez esse fato, aliado à preocupação de encontrar fórmulas que fornecessem apenas números primos, tenha levado Pierre de Fermat (1601-1658) a afirmar a recíproca desse resultado. Com efeito, em carta de 1640 dirigida a seu amigo Bernard Frenide de Bessy dizia, embora confessando não ter uma prova, que todos os números

$$F_n = 2^{(2^n)} + 1 \qquad (n \geqslant 0)$$

(hoje chamados números de Fermat — daí a notação F_n) são primos.

Como ele próprio só havia calculado F_0, F_1, F_2, F_3 e F_4 (todos primos) e certamente não teve condições de verificar a validade dessa afirmação para $n \geqslant 5$, mais tarde chegou a achar que estava errado. E, de fato, embora Fermat tivesse se notabilizado pelo acerto de várias conjecturas importantes, neste caso falhou. Em 1732 Leonard Euler (1707-1783), o maior matemático do século XVIII, provou que F_5 é divisível por 641 e portanto é composto. Curiosamente, para $n \geqslant 5$, todos os casos decididos até hoje contraditaram a conjectura de Fermat. Por exemplo, sabe-se atualmente que F_n é composto para todo n, $5 \leqslant n \leqslant 16$.

Mas apesar disso o assunto não morreria por aí. Em 1796, mais de um século e meio depois da citada carta de Fermat, o matemático Karl F. Gauss (1777-1855) provou que um polígono regular de n lados é construtível com régua e compasso se, e somente se

$$n = 2^k (2 > 1) \text{ ou } n = 2^k p_1 p_2 \ldots p_r \ (k \geqslant 0)$$

onde $r \geqslant 1$ e os p_i são primos de Fermat, distintos entre si quando $r \geqslant 2$ — um fato com toda a certeza insuspeitado por Fermat.

Vale registrar que nessa ocasião Gauss não atingira ainda os 20 anos de idade e que, desde os tempos de Euclides (séc. III a.C.), nenhuma contribuição significativa fora dada a esse assunto.

EXERCÍCIOS

87. (Fuvest-84) Sejam $m = 2^6 \cdot 3^3 \cdot 5^2$, $n = 2^r \cdot 3^s \cdot 5^t$ e $p = 2^5 \cdot 5^4$.

a) Quantos divisores de m são múltiplos de 100?

b) Escreva as condições que devem satisfazer r, s e t para que n seja divisor comum de m e p.

88. Decomponha em fatores primos:

a) 51 262 b) 20 305 c) 123 057

89. Dados a, b, c $\in$ IN, através de sua decomposição canônica:
$a = 3^2 \cdot 19 \cdot 71^2$, $b = 2 \cdot 3^5 \cdot 19 \cdot 61$, $c = 2^4 \cdot 19^2 \cdot 71$, ache:

i) mdc (a, b) iii) mdc (a, b, c) v) mmc (a, b)
ii) mdc (b, c) iv) mmc (a, c)

90. (Magistério — 1º e 2º graus — SP-86) Sejam a e b números naturais, não primos entre si, cujo produto é 420. O máximo divisor comum de a e b é:

a) 1 b) 2 c) 3 d) 5 e) 7

91. Verifique se são primos ou não os números: 269, 287 e 409.

92. Ache três pares de números a, b $\in$ IN de modo que mdc(a, b) = 11 e mmc(a, b) $= 2^2 \cdot 11^2 \cdot 29^3$.

93. a) Mostre que todo número primo é da forma 4k + 1 ou 4k + 3.
b) Mostre que todo número primo é da forma 6k + 1 ou 6k + 5.

Resolução de a: Pelo algoritmo da divisão, aplicado a um número a $\in$ IN (dividendo) e a 4 (divisor): a = 4k, a = 4k + 1, a = 4k + 2 e a = 4k + 3. O primeiro e o segundo casos representam números compostos (são múltiplos de 2). Restam: a = 4k + 1 ou a = 4k + 3.

94. (Fuvest-77) Sejam a e b números naturais e p um número primo.

a) Se p divide $a^2 + b^2$ e p divide a, então p divide b.

b) Se p divide ab, então p divide a e divide b.

c) Se p divide a + b, então p divide a e divide b.

d) Se a divide p, então a é primo.

e) Se a divide b e p divide b, então p divide a. Qual dessas afirmações é verdadeira?

95. Se a soma de dois números naturais não nulos é um número primo, prove que esses números são primos entre si.

96. Se m = mmc (a, b), mostre que mdc (a + b, m) = mdc (a, b), sempre que a, b > 0.

Resolução: Seja d = mdc (a, b). Como mdc $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, então mdc $\left(\frac{a}{d} + \frac{b}{d}, \frac{a}{d} \cdot \frac{b}{d}\right) = 1$ (ver exemplo 11). Daí (propos. 3): mdc $\left(a + b, \frac{ab}{d}\right) = d$. Ou seja:

$$\text{mdc } (a + b, m) = d = \text{mdc } (a, b)$$

97. Por meio do crivo de Eratóstenes, ache todos os números naturais primos menores que 150.

98. Mostre que todo primo da forma 3n + 1 é necessariamente da forma 6m + 1.

99. Prove que todo número natural do tipo 3n + 2 admite um divisor do mesmo tipo.

Resolução: Os divisores primos de 3n + 2 são de dois tipos: 3r + 1 e 3s + 2. Se todos fossem do primeiro tipo, então:

$$3n + 2 = (3r_1 + 1)(3r_2 + 1) \ldots (3r_k + 1) = 3r + 1$$

o que não é possível.

100. Se p é um número natural primo e se a é um inteiro tal que 1 < a < p, prove que p divide $\binom{p}{a}$.

Lembrete: $\binom{p}{a} = \dfrac{p(p-1)\ldots(p-a+1)}{a!}$

101. Seja $n \geqslant 2$. Mostre que entre n e n! existe um primo p.

Sugestão: Considere n! − 1.

102. Sejam a, b e p números naturais, sendo p primo. Se mdc (ab, p) = 1, prove que: $p^{k+1} | (ap^k + bp^s) \iff k = s$ e $p | (a + b)$.

103. Se a e b são números naturais primos entre si, prove que a^n, b^m também o são, para quaisquer n, m $\in \mathbb{N}$.

Resolução: Vamos supor mdc $(a^n, b^m) \neq 1$. Então a^n e b^m admitem um divisor primo comum p. Se $n = 1$, então $p|a$; se $n > 1$, então $p|a$ ou $p|a^{n-1}$; por indução: $p|a$. Analogamente $p|b$. Absurdo.

104. Se $2^n - 1$ $(n \geqslant 2)$ é primo, prove que n também é primo.

Sugestão: Se n fosse composto, $n = rs$ $(r, s > 1)$, então $2^n - 1$ poderia ser fatorado não trivialmente (em fatores maiores que 1) segundo a fórmula do exercício 25-d.

105. Qual o menor número natural que admite 15 divisores? E o menor que admite 20 divisores?

106. Prove que um número natural não nulo tem um número ímpar de divisores se, e somente se, esse número é quadrado perfeito.

107. Mostre que $\tau(n) = 2$ se, e somente se, n é primo.

108. Determine α e β para que $n = 2^3 \cdot 5^\alpha \cdot 7^\beta$ tenha 84 divisores.

109. Seja n um número natural livre de quadrados (n não é divisível por nenhum quadrado perfeito). Se r é o número de fatores primos de n, mostre que $\tau(n) = 2^r$.

Resolução: Sendo n livre de quadrados e sendo $p_1, \ldots, p_r$ seus fatores primos, então $n = p_1 p_2 \ldots p_r$. Logo, $\tau(n) = (1 + 1)(1 + 1) \ldots$ $\ldots (1 + 1) = 2^r$.

110. Mostre que todo número natural $n > 2$ pode ser escrito $n = 2^k \cdot m$, onde $k \geqslant 0$ e m é ímpar.

9. A função sigma e os números perfeitos

9.1 A função sigma

Costuma-se indicar por $\sigma(n)$ a soma de todos os divisores de um número $n \in \mathbb{N}^*$. Por exemplo, se $n = 12$, como os divisores de 12 são 1, 2, 3, 4, 6 e 12, então:

$$\sigma(n) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

Se p é primo, como os únicos divisores de p são 1 e p, então $\sigma(p) = 1 + p$. Se p é primo e $\alpha \in \mathbb{N}$, então, de acordo com a propriedade **III**, 8.1, os divisores de p^α são os $\alpha + 1$ números

$$1, p, p^2, \ldots, p^\alpha$$

Portanto:

$$\sigma(p^\alpha) = 1 + p + \ldots + p^\alpha = \frac{(p^\alpha + p^{\alpha-1} + \ldots + p + 1)(p - 1)}{p - 1} = \frac{p^{\alpha+1} - 1}{p - 1}$$

É claro que $n \to \sigma(n)$ é uma função definida e com valores em $\mathbb{N}^*$. Estabeleceremos a seguir uma fórmula que fornece $\sigma(n)$ uma vez conhecida a decomposição de n em fatores primos.

PROPOSIÇÃO 11 Seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, onde $r \geqslant 1$, cada fator p_i é primo e $p_i \neq p_j$ sempre que $i \neq j$. Então:

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \ldots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

Demonstração (por indução sobre r): Como já vimos a proposição é válida para $r = 1$. Seja $r > 1$ e admitamos que seja verdadeira para $r - 1$. Supondo

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

conforme o enunciado, façamos

$$p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_r^{\alpha_r} = m$$

e sejam $1 = d_1, d_2, \ldots, d_k = m$ os divisores de m. Como um divisor de n é necessariamente do tipo

$$p_1^{\beta_1} \cdot p_2^{\beta_2} \ldots p_r^{\beta_r} \; (0 \leqslant \beta_i \leqslant \alpha_i;\ i = 1, 2, \ldots, r)$$

(devido a **III**, 8.1), então esses divisores são:

$$p_1^{\beta_1} \cdot d_i \; (0 \leqslant \beta_1 \leqslant \alpha_1;\ i = 1, 2, \ldots, k)$$

Logo,

$$\sigma(n) = \sum_{\beta_1=0}^{\alpha_1} \sum_{i=1}^{k} p_1^{\beta_1} d_i = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right)\left(\sum_{i=1}^{k} d_i\right) = \sigma(p_1^{\alpha_1})\,\sigma(m) =$$

$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \sigma(m)$$

Mas, pela hipótese de indução:

$$\sigma(m) = \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

Donde:

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}. \qquad \blacksquare$$

Exemplo 16: Como $20 = 2^2 \cdot 5$, então

$$\sigma(20) = \frac{2^3 - 1}{2 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 7 \cdot 6 = 42$$

é a soma dos divisores de 20.

9.2 Sobre números perfeitos

Já falamos, no capítulo I, sobre os números perfeitos, introduzidos na Matemática pelos pitagóricos. Usando a função σ pode-se caracterizar um número perfeito $n \in \mathbb{N}^*$ pela igualdade

$$\sigma(n) - n = n \text{ (ou } \sigma(n) = 2n).$$

De fato, se n é perfeito, então a soma de seus divisores, excluído ele próprio, deve ser n.

Os gregos, porém, segundo se pode inferir da *Introductio Arithmetica*, de Nicômaco de Gerasa (viveu em torno do ano 100 d.C.), só conheciam os quatro primeiros números perfeitos: com a notação atual, $P_1 = 6$, $P_2 = 28$, $P_3 = 496$ e $P_4 = 8\,128$.

Mas Euclides, no seu *Elementos*, já provara que: "Se $2^k - 1$ é primo $(k > 1)$, então $n = 2^{k-1} \cdot (2^k - 1)$ é perfeito"(*). A demonstração deste fato pode ser feita observando que o número 2 não é fator primo de $2^k - 1$, já que este número obviamente é ímpar. Assim, conforme argumento empregado na demonstração da proposição anterior,

(*) Proposição 36 — livro IX.

$$\sigma(n) = \sigma(2^{k-1})\,\sigma(2^k - 1) = \frac{2^k - 1}{2 - 1} \cdot 2^k = 2[2^{k-1}(2^k - 1)] = 2n$$

onde usamos o fato de $2^k - 1$ ser primo (hipótese) e portanto $\sigma(2^k - 1) = 1 + 2^k - 1 = 2^k$.

Os quatro primeiros números perfeitos podem ser obtidos através dessa proposição, fazendo k = 2, 3, 5 e 7. O quinto número perfeito foi encontrado na primeira metade do século XVI por Hudalrichus Regius e corresponde a k = 13

$$P_5 = 2^{12} \cdot (2^{13} - 1) = 33 \cdot 350 \cdot 336$$

Em 1603, Pietro Cataldi encontrou P_6 e P_7, fazendo k = 17 e k = 19, respectivamente, na fórmula da citada proposição de Euclides.

Em 1644 Marin Mersenne (1588-1648) conjecturou que os números $M_p = 2^p - 1$ $(p \geqslant 1)$ são primos para p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257 e compostos para todos os outros primos $p < 257$. Mersenne, obviamente, não tinha, como ninguém na época, condições de verificar tal afirmação. Mas, com isso, os números do tipo

$$M_n = 2^n - 1 \; (n \geqslant 1)$$

passaram à história com o nome de ***números de Mersenne***.

O número M_{19} foi o maior primo de Mersenne conhecido até 1732 quando Euler provou que M_{31} é primo. Mas a conjectura de Mersenne continha cinco erros. Hoje sabemos que: M_{61} é primo, M_{67} é composto, M_{89} e M_{107} são primos e M_{257} é composto. Os recursos da computação eletrônica naturalmente têm facilitado a descoberta de números perfeitos. Por exemplo, foi através desse expediente que em 1983 Slowinski mostrou que M_{132049} é primo. O número perfeito associado a esse número de Mersenne é

$$P_{29} = 2^{132048}(2^{132049} - 1)$$

formado de aproximadamente 79 000 dígitos.

Euler provou a seguinte recíproca da já citada proposição 36 de Euclides: "Se n é um número perfeito par, então

$$n = 2^{k-1} \cdot (2^k - 1)$$

onde $k > 1$ e $2^k - 1$ é um número de Mersenne primo".

Mas duas questões cruciais sobre números perfeitos ainda permanecem em aberto:

- Há algum número perfeito que seja ímpar?
- O conjunto dos números perfeitos é finito ou infinito?

EXERCÍCIOS

111. Calcule $\sigma(n)$ para $n = 1, 2, \ldots, 10$.

112. Mostre que não são perfeitos os números:

a) $2^{15} \cdot (2^{16} - 1)$ b) 691

113. Prove que um número primo não pode ser perfeito.

114. Prove que:

a) Um número perfeito nunca é uma potência de um número primo.
b) Um número perfeito nunca é um quadrado perfeito.
c) Um número perfeito nunca é o produto de dois números primos ímpares.

Resolução de c): Vamos supor $n = pq$, onde p e q são primos ímpares, $p \neq q$ (o caso $p = q$ cai em b). Então:

$$\sigma(n) = \frac{p^2 - 1}{p - 1} \cdot \frac{q^2 - 1}{q - 1} = (p + 1)(p + 1) = 2n = 2pq$$

Daí segue que $pq = p + q + 1$. Mas é fácil provar que se p e q são números naturais $\geqslant 3$, então $pq > p + q + 1$ (por indução sobre q, por exemplo). Este absurdo mostra que não pode ocorrer $n = p \cdot q$, nas condições supostas.

115. Use o teorema de Euler já citado, segundo o qual todo número perfeito par é da forma $2^{k-1} \cdot (2^k - 1)$, onde $2^k - 1$ é primo, para provar que todo número perfeito par é um número triangular.

116. Um número natural se diz *abundante* se $\sigma(n) > 2n$ e *deficiente* se $\sigma(n) < 2n$.

a) Classifique em deficientes, perfeitos ou abundantes os números 1, 2, 3, ..., 15.
b) Ache todos os números deficientes e todos os abundantes da forma $2 \cdot 5^s$ $(s \geqslant 0)$.

117. Mostre que todo múltiplo de um número perfeito, diferente do próprio número e de zero, é abundante.

118. Se n é um número perfeito par e se $d | n$, $1 < d < n$, mostre que d é deficiente.

119. Se $n > 2$ e se $2n + 1$ é primo, prove que $a = 2n(2n + 1)$ é um número abundante.

Resolução: Levando em conta que $2n + 1$ é primo e que mdc $(2n, 2n + 1) = 1$, a argumentação usada para provar a proposição 11 permite escrever que:

$$\sigma(a) = \sigma(2n)\,\sigma(2n + 1) = \sigma(2n) \cdot (2n + 2)$$

Vamos supor $n = 2^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, onde $\alpha_i \geqslant 0$ $(i = 1, 2, \ldots, r)$ e $2, p_2, \ldots, p_r$ são os possíveis fatores primos de n. Então:

$$\sigma(2n) = (2^{\alpha_1+1} + 2^{\alpha_1} + \ldots + 1)(p_2^{\alpha_2} + \ldots + 1) \ldots (p_r^{\alpha_r} + \ldots + 1)$$

Neste produto o primeiro fator é $\geqslant 2^{\alpha_1+1} = 2 \cdot 2^{\alpha_1}$, o segundo $\geqslant p_2^{\alpha_2}, \ldots$, o último $\geqslant p_r^{\alpha_r}$. Logo $\sigma(2n) \geqslant 2n$ e então $\sigma(a) \geqslant (2n)(2n + 2) > a$.

120. Seja n um número perfeito. Prove que $\sum\limits_{d|n} \frac{1}{d} = 2$.

Nota: O somatório é estendido a todos os divisores de n (inclusive 1 e n) e a apenas estes números.

Resolução: Sejam $d_1, d_2, \ldots, d_r$ os divisores de n. Então $\frac{n}{d_1}, \ldots, \frac{n}{d_r}$ também são os divisores (todos) de n. De fato, como $n = \frac{n}{d_i} \cdot d_i$, então $\frac{n}{d_i}$ divide n $(i = 1, 2, \ldots, r)$; por outro lado, se $\frac{n}{d_i} = \frac{n}{d_j}$, então $d_i = d_j$. Logo:

$$\sum_{d|n} \frac{n}{d} = \sum_{d|n} d = 2n$$

do que resulta

$$n \sum_{d|n} \frac{1}{d} = 2n$$

e portanto

$$\sum_{d|n} \frac{1}{d} = 2$$

121. Use o resultado anterior para provar que se n é perfeito e $d | n$, $d \neq n$, então d não é perfeito.

122. Mostre que, para todo $n \in \mathbb{N}^*$, $n \leqslant \sigma(n) \leqslant n^2$.

10. Os ternos pitagóricos

No capítulo I já fizemos alguns comentários sobre os ternos pitagóricos. Lembremos que se trata dos ternos (a, b, c) de números naturais não nulos para os quais vale $a^2 + b^2 = c^2$. Logo, se (a, b, c) é um terno pitagórico, a, b e c indicam, respectivamente, os catetos e a hipotenusa de um triângulo retângulo. Aliás, desse fato e da grande ênfase dada pela escola pitagórica aos números (os naturais não nulos) vem a designação dada hoje em dia a esses ternos. Algebricamente os ternos pitagóricos são soluções da equação sobre $\mathbb{N}$: $x^2 + y^2 = z^2$. Mostramos no capítulo I que os próprios pitagóricos chegaram à fórmula

$$\left(m, \frac{m^2 - 1}{2}, \frac{m^2 + 1}{2}\right)$$

que, para m ímpar, fornece infinitas soluções dessa equação (embora não todas). Nosso objetivo agora é obter todos os ternos pitagóricos.

É interessante, de passagem, alinhavar alguns comentários sobre a equação geral $x^n + y^n = z^n$ $(n \geqslant 1)$. Obviamente essa equação tem infinitas soluções em $\mathbb{N}^3 = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ quando n = 1. O mesmo ocorre, como já observamos, para n = 2. Em 1637 Fermat anotou, às margens de uma tradução para o latim que possuía da *Arithmetica* de Diofanto (séc. III d.C., provavelmente), que havia conseguido uma demonstração "verdadeiramente maravilhosa" de que, para $n \geqslant 3$, $x^n + y^n = z^n$ só admite, em $\mathbb{N}^3$, a solução trivial (0, 0, 0). Porém, concluiu ele: "... a margem não é grande o suficiente para contê-la". Esse resultado, hoje conhecido como "grande teorema de Fermat" ou "último teorema de Fermat", até agora não foi provado totalmente.

O próprio Fermat conseguiu uma demonstração para n = 4, ou seja, que $x^4 + y^4 = z^4$ só admite a solução trivial em $\mathbb{N}^3$. A demonstração para n = 3 foi feita por Euler em 1738. Para n = 5 o mérito coube a Adrien-Marie Legendre (1752-1833) e para n = 7 a Gabriel Lamé (1795-1870).

Sabe-se hoje, através de computadores eletrônicos, que não há soluções não triviais de $x^n + y^n = z^n$ em $\mathbb{N}^3$ para $3 \leqslant n < 125\,000$, embora muitos desses casos já tivessem sido resolvidos convencionalmente.

O último e importante resultado a respeito foi obtido por Gerd Faltings em 1983 ao provar a chamada conjectura de Mordell que há 60 anos desafiava os pesquisadores de teoria dos números (Matemática universitária — nº 1 — 1985). É que, do resultado obtido por Faltings, decorre que para $n \geqslant 3$ a equação $x^n + y^n = z^n$ tem no máximo um número finito de soluções em $\mathbb{N}^3$.

DEFINIÇÃO 6 Um terno pitagórico (a, b, c) se diz *primitivo* se mdc(a, b, c) = 1.

A importância dessa definição está no seguinte fato: um terno

$(a, b, c) \in \mathbb{N}^3$ é pitagórico se, e somente se, existe $d \in \mathbb{N}$ e existe um terno pitagórico primitivo (a_1, b_1, c_1) tal que $(a, b, c) = (da_1, db_1, dc_1) = d(a_1, b_1, c_1)$. De fato, seja (a, b, c) pitagórico e seja d = mdc (a, b, c). Então $a = da_1$, $b = db_1$, $c = dc_1$, onde $a_1, b_1, c_1 \in \mathbb{N}$ e mdc $(a_1, b_1, c_1) = 1$ (conforme generalização óbvia do corolário 1, proposição 3). Como $a^2 + b^2 = c^2$, então $d^2a_1^2 + d^2b_1^2 = d^2c_1^2$, do que resulta $a_1^2 + b_1^2 = c_1^2$. Logo (a_1, b_1, c_1) é pitagórico primitivo. A recíproca é imediata.

Assim, para determinar todos os ternos pitagóricos, basta encontrar aqueles que são primitivos.

LEMA 1 Se (a, b, c) é um terno pitagórico primitivo, então mdc (a, b) = mdc (b, c) = mdc (a, c) = 1.

Demonstração: Suponhamos, por exemplo, mdc (a, c) = d > 1. Daí a = dr e c = ds, onde $r, s \in \mathbb{N}$. Como $a^2 + b^2 = c^2$, então $d^2r^2 + b^2 = d^2s^2$ e portanto $d^2 | b^2$. Donde (exemplo 12), d|b. Assim d|a, d|b e d|c, o que é absurdo. ■

LEMA 2 Seja (a, b, c) um terno pitagórico primitivo. Então a e b não podem ser ambos ímpares.

Demonstração: Suponhamos a = 2r + 1 e b = 2s + 1. Então $a^2 + b^2 = 4(r^2 + s^2 + r + s) + 2 = 4k + 2$ (par). Mas isso impede c de ser ímpar. De fato, se c fosse ímpar, o mesmo ocorreria com c^2 e teríamos o seguinte absurdo:

$$\text{ímpar} \rightarrow c^2 = a^2 + b^2 \leftarrow \text{par}$$

Por outro lado, se c fosse par, c = 2n, então

$$4n^2 = c^2 = a^2 + b^2 = 4k + 2$$

do que também resulta um absurdo, ou seja

$$\text{par} \rightarrow 2n^2 = 2k + 1 \leftarrow \text{ímpar}$$

Donde a e b não são ímpares simultaneamente. ■

LEMA 3 Sejam a, b, $c \in \mathbb{N}^*$ números tais que mdc (a, b) = 1 e $ab = c^2$. Então a e b são quadrados perfeitos.

Demonstração: Todo fator primo p de a é também fator primo de c^2 mas não é fator primo de b, pois mdc (a, b) = 1. Mas em c^2 todo fator primo tem expoente par. Logo o expoente de p em a é par (o mesmo que figura em c^2). Se todos os expoentes dos fatores primos de a têm expoente par, então obviamente a é quadrado perfeito. A mesma argumentação vale para b. ■

TEOREMA 4 Seja (a, b, c) um terno pitagórico primitivo em que a é par. Então existem u, v $\in$ IN*, primos entre si, um par outro ímpar, u > v, de maneira que

$$a = 2uv,\ b = u^2 - v^2 \text{ e } c = u^2 + v^2$$

Reciprocamente, todo terno $(2uv, u^2 - v^2, u^2 + v^2)$, onde u e v satisfazem as condições enunciadas, é pitagórico primitivo.

Demonstração:

i Seja (a, b, c) pitagórico, primitivo, e admitamos a par. Se b fosse par, o mesmo ocorreria com $c^2 = a^2 + b^2$ e portanto também c seria par, o que é impossível, pois (a, b, c) é primitivo. Logo b é ímpar e $c^2 = a^2 + b^2$ também; daí c também é ímpar. Como então

$$a^2 = c^2 - b^2 = (c - b)(c + b)$$

onde c − b e c + b são pares, ambos os membros dessa igualdade são divisíveis por 4, do que resulta

$$\left(\frac{a}{2}\right)^2 = \frac{c-b}{2} \cdot \frac{c+b}{2}$$

Como porém

$$\frac{c-b}{2} + \frac{c+b}{2} = c \quad \text{e} \quad \frac{c+b}{2} - \frac{c-b}{2} = b$$

e mdc (b, c) = 1, então

$$\text{mdc}\left(\frac{c-b}{2}, \frac{c+b}{2}\right) = 1$$

já que todo divisor de $\frac{c+b}{2}$ e $\frac{c-b}{2}$ é divisor também de sua soma e de sua diferença.

O lema 3 garante então a existência de u, v $\in$ IN* de maneira que

$$\frac{c+b}{2} = u^2 \quad \text{e} \quad \frac{c-b}{2} = v^2$$

onde u > v. Daí

$$c + b = 2u^2 \quad \text{e} \quad c - b = 2v^2$$

e portanto $c = u^2 + v^2$ e $b = u^2 - v^2$. Mas

$a^2 = c^2 - b^2 = (u^2 + v^2)^2 - (u^2 - v^2)^2 = u^4 + 2u^2v^2 + v^4 - u^4 + 2u^2v^2 - v^4 =$
$= 4u^2v^2$. Donde a = 2uv.

Como todo fator comum a u e v é fator comum a b e c (pois $c = u^2 + v^2$ e

$b = u^2 - v^2$) e como mdc (b, c) = 1, então u e v são primos entre si. Finalmente, se u e v fossem ambos pares ou ambos ímpares, as igualdades $c = u^2 + v^2$ e $b = u^2 - v^2$ obrigariam c e b a serem ambos pares, o que não é possível.

ii Observando que

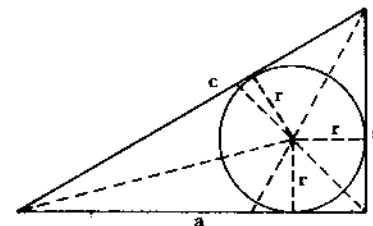
$(2uv)^2 + (u^2 - v^2)^2 = 4u^2v^2 + u^4 - 2u^2v^2 + v^4 =$
$= u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2$

então pode-se concluir que $(2uv, u^2 - v^2, u^2 + v^2)$ é pitagórico. Por outro lado, como u é par (ímpar) e v é ímpar (par) então $u^2 - v^2$ e $u^2 + v^2$ são ímpares e portanto o fator 2 de 2uv não é fator comum aos termos de $(2uv, u^2 - v^2, u^2 + v^2)$.

Vamos supor, por último, que um primo p > 2 fosse fator comum a esses termos. Como p|2uv e p > 2 então p|u ou p|v; como estamos supondo que $p|(u^2 + v^2)$, então chegamos à conclusão que p|u e p|v, o que não é possível. Logo, efetivamente, $(2uv, u^2 - v^2, u^2 + v^2)$, conforme o enunciado, é um terno pitagórico primitivo. ■

Exemplo 17: Construiremos agora uma tabela parcial de ternos pitagóricos. Nas duas primeiras colunas colocaremos pares u, v $\in$ IN*, u > v, primos entre si, um desses elementos par e o outro ímpar. Nas duas colunas seguintes aparecerão os catetos e na última as hipotenusas respectivas.

u	v	$a = 2uv$	$b = u^2 - v^2$	$c = u^2 + v^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	3	30	16	34

Exemplo 18: Um triângulo retângulo se diz *pitagórico* se as medidas de seus lados são números naturais. Mostremos que o raio do círculo inscrito num triângulo pitagórico também é um número natural.

A área do triângulo é dada por:

$$A = \frac{1}{2} ab = \frac{1}{2} ra + \frac{1}{2} rb + \frac{1}{2} rc = \frac{1}{2} r(a + b + c)$$

Logo:

$$ab = r(a + b + c)$$

Mas, considerando o teorema 4 e as considerações que o precedem:

$$a = 2kuv, \; b = k(u^2 - v^2) \text{ e } c = k(u^2 + v^2)$$

onde k, u e v são convenientes números naturais não nulos. Então:

$$ab = (2kuv)\,k(u^2 - v^2) = r(a + b + c) =$$
$$= r[2kuv + k(u^2 - v^2) + k(u^2 + v^2)]$$

ou

$$2k^2uv(u - v)(u + v) = r[2kuv + 2ku^2] = 2rku(v + u)$$

Daí, cancelando os fatores comuns

$$kv(u - v) = r$$

o que garante nossa afirmação, pois $k, u, v \in \mathbb{N}$.

EXERCÍCIOS

123. Determine os ternos pitagóricos primitivos correspondentes aos seguintes pares de números naturais u, v, conforme o teorema 4:

a) $u = 9, v = 5$ c) $u = 10, v = 7$
b) $u = 11, v = 10$ d) $u = 11, v = 6$

124. Ache todos os ternos pitagóricos primitivos das formas:

a) (12, b, c) b) (a, 8, c)

125. Seja (a, b, c) um terno pitagórico no qual a e c são números naturais consecutivos. Mostre que $a = 2t(t + 1)$, $b = 2t + 1$ e $c = 2t(t + 1) + 1$, para algum $t \in \mathbb{N}$ e que, portanto, (a, b, c) é primitivo.

126. Mostre que (3, 4, 5) é o único terno pitagórico primitivo cujos termos são números naturais consecutivos.

127. Seja (a, b, c) um terno pitagórico tal que $c = b + 2$. Prove que existe $r \in \mathbb{N}$ tal que $a = 2r$, $b = r^2 - 1$ e $c = r^2 + 1$. Esse terno é primitivo?

128. Se (a, b, c) é um terno pitagórico, prove que $3 \nmid a$ ou $3 \nmid b$.

Resolução: Vamos supor que $3 \nmid a$ e $3 \nmid b$. Então: ($a = 3t + 1$ ou $a = 3t + 2$) e ($b = 3r + 1$ ou $b = 3r + 2$). Supondo, por exemplo, $a = 3t + 2$ e $b = 3r + 1$, então $a^2 + b^2 = (3t + 2)^2 + (3r + 1)^2 = 3q + 2$, onde $q = 3t^2 + 3r^2 + 4t + 2r + 1$. Assim, teríamos que ter $c^2 = 3q + 2$. Mas isso não é possível, como se pode verificar para todas as formas possíveis de c: $c = 3s$, $c = 3s + 1$ ou $c = 3s + 2$. De fato, se por exemplo $c = 3s + 2$, então $c^2 = 9s^2 + 12s + 4 = 3u + 1$.
Para os demais casos, o procedimento é o mesmo.

129. Seja (a, b, c) um terno pitagórico cujos termos, na ordem em que aparecem, formam uma progressão aritmética. Prove que existe $r \geqslant 1$ de modo que $a = 3r$, $b = 4r$ e $c = 5r$.

130. Seja (a, b, c) um terno pitagórico tal que b é ímpar. Prove que $4 | a$.

131. Se (a, b, c) é um terno pitagórico primitivo, mostre que um de seus termos é necessariamente múltiplo de 5.

132. Se (a, b, c) é um terno pitagórico primitivo, prove que $12 | ab$ e $60 | abc$.

Resolução: Como (a, b, c) é primitivo, podemos supor $a = 2uv$, $b = u^2 - v^2$ e $c = u^2 + v^2$, onde $u > v$, mdc (u, v) = 1, v é ímpar e u é par (ou vice-versa). Supondo u par e considerando que $2u | a$ então $4 | a$. Mas $3 | a$ ou $3 | b$, conforme exercício 128. Levando em conta que mdc (3, 4) = 1, podemos concluir então que $12 | ab$. Para concluir que $60 | abc$, basta levar em conta o exercício anterior.

133. Seja (a, a + 1, c) um terno pitagórico. Se T_k indica o k-ésimo número triangular, isto é, $T_k = \frac{k(k + 1)}{2}$, prove que $(T_{2a}, T_{2a+1}, (2a + 1)c)$ é também um terno pitagórico.

11. A seqüência de Fibonacci

11.1 Leonardo de Pisa

Leonardo de Pisa (1180-1250), mais conhecido como Fibonacci (o que significa "filho de Bonaccio"), é considerado o matemático mais capaz e original do Ocidente no período medieval. Sua obra mais famosa é o *Liber abaci*, de 1202. Apesar do título, cuja tradução literal é "Livro do ábaco", uma das

preocupações centrais desse trabalho era ensinar o uso dos numerais indo-arábicos — cujo conhecimento até então, na Europa, se limitava praticamente aos mosteiros.

Mas não é o mérito dessa obra, e de outros tratados que deixou, o motivo principal de Fibonacci ser lembrado ainda hoje. Ocorre que, talvez para amenizar a leitura do seu *Liber abaci*, ou para torná-la mais interessante, Fibonacci incluiu no livro alguns problemas curiosos e estimulantes, dentre os quais um veio a se tornar especialmente importante:

"Um homem põe um casal de coelhos dentro de um cercado. Quantos pares de coelhos serão produzidos num ano, se a natureza desses coelhos é tal que a cada mês um casal gera um novo casal, que se torna produtivo a partir do segundo mês?"

Ao fim de um mês haverá dois casais (o casal adulto com o qual se começou e um jovem), ao fim do segundo mês haverá três casais (dois adultos e um jovem), ao fim do terceiro haverá cinco casais (três adultos e dois jovens), e assim por diante. Em geral, se ao fim de um certo mês há r casais adultos e s jovens, ao final do mês seguinte haverá r + s casais adultos e r jovens e ao final do próximo 2r + s casais adultos e r + s jovens. Ou seja, o número de casais jovens, ao fim de um certo mês, a partir do terceiro, é igual à soma do número de casais jovens ao final dos dois meses anteriores.

Assim, se f_n indicar o número de casais jovens ao final do enésimo mês, então

$$f_1 = 1,\ f_2 = 1,\ f_3 = 1 + 1 = 2,\ f_4 = 1 + 2 = 3,\ f_5 = 2 + 3 = 5,\ f_6 = 3 + 5 = 8,\ \ldots$$

No século passado o matemático francês Edouard Lucas deu a $(f_n) = (1, 1, 2, 3, 5, 8, \ldots)$ o nome de *seqüência de Fibonacci*, designação que acabou sendo adotada universalmente e, assim, consagrando o nome de Fibonacci. Os termos dessa seqüência são chamados *números de Fibonacci*. É claro que (f_n) pode ser definida pela seguinte fórmula recursiva:

$$f_1 = f_2 = 1 \quad \text{e} \quad f_{n+1} = f_{n-1} + f_n \quad (n \geqslant 2)$$

As considerações que fizemos nos permitem concluir também que se $g_n = f_{n+1}$ $(n = 1, 2, \ldots)$, então g_n indica o número de adultos ao final do enésimo mês.

Mas é claro que a seqüência de Fibonacci não teria despertado tanta atenção se não fosse dotada de propriedades tão interessantes e não se mostrasse tão rica em aplicações. Nos parágrafos seguintes focalizaremos algumas dessas propriedades, especialmente as de cunho aritmético. Ao leitor interessado em ter uma idéia de algumas das possíveis aplicações dos números de Fibonacci, recomendamos a leitura do parágrafo 8.5 do texto [3] da bibliografia.

11.2 Propriedades gerais

I Para todo $n \geqslant 1$: $f_1 + f_2 + \ldots + f_n = f_{n+2} - 1$

Prova (por indução):

$n = 1$: $f_1 = f_3 - 1$ (verdadeira)

Vamos supor $r \geqslant 1$ e $f_1 + f_2 + \ldots + f_r = f_{r+2} - 1$

$n = r + 1$: $f_1 + \ldots + f_r + f_{r+1} = f_{r+2} - 1 + f_{r+1} = f_{r+3} - 1$ ■

II Para todo $n \geqslant 1$: $f_1^2 + f_2^2 + \ldots + f_n^2 = f_n f_{n+1}$

Prova (por indução):

$n = 1$: $f_1^2 = f_1 f_2$ (verdadeira)

Seja $r \geqslant 1$ e suponhamos $f_1^2 + \ldots + f_r^2 = f_r f_{r+1}$

$n = r + 1$: $f_1^2 + \ldots + f_r^2 + f_{r+1}^2 = f_r f_{r+1} + f_{r+1}^2 = f_{r+1}(f_r + f_{r+1}) = f_{r+1} f_{r+2}$ ■

III Se $m \geqslant 1$ e $n > 1$, então $f_{n+m} = f_{n-1} f_m + f_n f_{m+1}$

Prova (por indução sobre m):

$m = 1$: $f_{n+1} = f_{n-1} f_1 + f_n f_2 = f_{n-1} + f_n$ (verdadeira)

$m = 2$: $f_{n+2} = f_{n-1} f_2 + f_n f_3 = f_{n-1} + 2f_n = (f_{n-1} + f_n) + f_n = f_n + f_{n+1}$ (verdadeira)

Seja $r > 2$ e suponhamos a propriedade verdadeira para todo k, $2 \leqslant k < r$, e para todo $n > 1$. Esta suposição, mais o fato de que a propriedade vale também para $k = 1$, nos garante que:

$$f_{n+(r-2)} = f_{n-1} f_{r-2} + f_n f_{r-1}$$

e

$$f_{n+(r-1)} = f_{n-1} f_{r-1} + f_n f_r$$

Somando membro a membro essas igualdades e levando em conta a fórmula recursiva que define (f_n):

$$f_{n+r} = f_{n-1} f_r + f_n f_{r+1}$$

Ou seja, a fórmula vale também para r, sempre que $n > 1$. O segundo princípio de indução nos garante então que vale para todo $m \geqslant 1$ e qualquer $n > 1$. ■

COROLÁRIO Para todo $n > 1$: $f_{2n} = f_{n+1}^2 - f_{n-1}^2$

Prova: Façamos m = n na fórmula dada pela propriedade anterior.

Então:

$$f_{2n} = f_{n-1}f_n + f_nf_{n+1} = f_n(f_{n-1} + f_{n+1})$$

Mas

$$f_n = f_{n+1} - f_{n-1}$$

Logo

$$f_{2n} = (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) = f^2_{n+1} - f^2_{n-1}$$ ■

11.3 Propriedades aritméticas

IV Dois números de Fibonacci consecutivos f_n e f_{n+1} são primos entre si.

Prova: Seja $d = \text{mdc}(f_n, f_{n+1})$. Como f_n e f_{n+1} são maiores que zero, o mesmo ocorre com d. O fato de d ser divisor de f_n e f_{n+1} implica que $d|f_{n-1}$ pois $f_{n-1} = f_{n+1} - f_n$. Dividindo f_n e f_{n-1}, então d divide f_{n-2}. Prosseguindo nesse raciocínio chegaremos à conclusão que $d|f_2$. Então $d = 1$, pois $f_2 = 1$. ■

Nota: Consideremos os números de Fibonacci f_{n+1} e f_{n+2} que já sabemos serem primos entre si. Mas se aplicássemos o processo das divisões sucessivas a esses números obteríamos:

$$f_{n+2} = f_{n+1} \cdot 1 + f_n$$
$$f_{n+1} = f_n \cdot 1 + f_{n-1}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_4 = f_3 \cdot 1 + f_2$$
$$f_3 = f_2 \cdot 2 + 0$$

Isso mostra que seriam necessárias n divisões sucessivas para se chegar ao máximo divisor comum $f_2 = 1$ de f_{n+2} e f_{n+1}.

Logo, para todo $n > 0$, existem inteiros a e b tais que são necessárias exatamente n divisões sucessivas para se calcular mdc (a, b) através do algoritmo da divisão.

V Se $m|n$, então $f_m|f_n$.

Prova: Por hipótese $n = mr$, para algum $r \in \mathbb{N}$. Procederemos por indução sobre r.

Se $r = 1$, então $m = n$ e é imediato que $f_m|f_n$.
Seja $r \geqslant 1$ e admitamos que $f_m|f_{mr}$.
Então, levando em conta a relação fornecida por **III**:

$$f_{m(r+1)} = f_{mr+m} = f_{mr-1} \cdot f_m + f_{mr} \cdot f_{m+1}$$

Como $f_m|f_{mr-1} \cdot f_m$ e $f_m|f_{mr} \cdot f_{m+1}$ (pois, pela hipótese de indução, divide f_{mr}), então f_m divide a soma desses dois produtos. Ou seja: $f_m|f_{m(r+1)}$. ■

VI Se $d = \text{mdc}(m, n)$, então $\text{mdc}(f_m, f_n) = f_d$.

Prova: Mostremos primeiro que se $m = nq + r$, então $\text{mdc}(f_m, f_n) = \text{mdc}(f_n, f_r)$.
Observando a hipótese feita e levando em conta **III**:

$$\text{mdc}(f_m, f_n) = \text{mdc}(f_{nq+r}, f_n) = \text{mdc}(f_{nq-1} \cdot f_r + f_{nq} \cdot f_{r+1}, f_n)$$

Considerando porém que $\text{mdc}(a, b) = \text{mdc}(a + c, b)$, sempre que $b|c$ (exercício 74), e ainda que $f_n|f_{nq}$ (propriedade **V**), chegamos a:

$$\text{mdc}(f_m, f_n) = \text{mdc}(f_{nq-1} \cdot f_r, f_n)$$

Mostremos que f_{nq-1} e f_n são primos entre si. De fato, se d é um divisor comum a esses dois números, então $d|f_{nq-1}$ e $d|f_{nq}$ (devido a **V**). Daí d é um divisor da soma $f_{nq-1} + f_{nq} = f_{nq+1}$. Mas se $d|f_{nq}$ e $d|f_{nq+1}$, então **IV** nos assegura que $d = 1$.
Ora, se $\text{mdc}(f_{nq-1}, f_n) = 1$, então $\text{mdc}(f_r, f_n) = \text{mdc}(f_{nq-1} \cdot f_r, f_n)$ (exercício 76). Donde

$$\text{mdc}(f_m, f_n) = \text{mdc}(f_n, f_r)$$

Assim, supondo $m > n$, e aplicando o processo das divisões sucessivas para se chegar a $d = \text{mdc}(m, n)$:

$$m = nq_1 + r_1 \quad (r_1 < n)$$
$$n = r_1q_2 + r_2 \quad (r_2 < r_1)$$
$$r_1 = r_2q_3 + r_3 \quad (r_3 < r_2)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{n-2} = r_{n-1}q_n + r_n \quad (r_n < r_{n-1})$$
$$r_{n-1} = r_nq_{n+1} \quad (\text{onde } r_n = d)$$

o uso repetido do resultado anterior a cada uma das igualdades anteriores nos levará a concluir que

$$\text{mdc}(f_m, f_n) = \text{mdc}(f_{r_{n-1}}, f_d)$$

Como $d \mid r_{n-1}$ e portanto, em virtude de **V**, $f_d \mid f_{r_{n-1}}$, então:

$\text{mdc}(f_m, f_n) = f_d$. ■

COROLÁRIO (recíproco de **V**): Se $f_m \mid f_n$ e $m \neq 2$, então $m \mid n$.

Prova: De $f_m \mid f_n$ decorre que $\text{mdc}(f_m, f_n) = f_m$. Mas, devido a **VI**:

$$\text{mdc}(f_m, f_n) = f_d$$

onde $d = \text{mdc}(m, n)$. Logo $f_m = f_d$. Se $m > 2$, então $f_m \geqslant 2$, daí $f_d \geqslant 2$ e portanto $d > 2$, o que implica $m = d$. Assim, para todo $m \neq 2$ vale a igualdade $m = d$, o que obviamente acarreta $m \mid n$. ■

Os resultados com que já contamos nos permitem chegar a outras propriedades interessantes, como os "critérios de divisibilidade" que exporemos a seguir. Por critérios de divisibilidade entendemos, no caso, condições necessárias e suficientes para que um certo número de Fibonacci seja divisível por um dado número.

- Um número de Fibonacci é divisível por 2 (portanto é par) se, e somente se, seu índice é divisível por 3.
- Um número de Fibonacci é divisível por 3 se, e somente se, seu índice é divisível por 4.
- Um número de Fibonacci é divisível por 4 se, e somente se, seu índice é divisível por 6.

Demonstraremos em seguida o primeiro desses critérios. Sugerimos ao leitor a demonstração dos outros dois, além da procura de outros critérios.

Prova:

⇒ Por hipótese

$$f_3 = 2 = \text{mdc}(f_n, 2) = \text{mdc}(f_n, f_3) = f_{\text{mdc}(n,3)}$$

Logo

$$\text{mdc}(n, 3) = 3$$

o que implica $3 \mid n$.

⇒ Como $3 \mid n$, por hipótese, então $n = 3q$ e portanto

$$f_n = f_{3q}$$

Mas, devido a **V**:

$$f_3 \mid f_{3q}$$

Como $f_3 = 2$ e $f_{3q} = f_n$, então $2 \mid f_n$. ■

EXERCÍCIOS

134. Ache $\text{mdc}(f_9, f_{12})$, $\text{mdc}(f_{15}, f_{20})$ e $\text{mdc}(f_{24}, f_{36})$.

135. Verdadeiro ou falso: se $s = \text{mmc}(m, n)$, então $f_s = \text{mmc}(f_m, f_n)$? Justifique.

136. Ache os números de Fibonacci que são divisores de f_{16} e f_{30}.

137. Verdadeiro ou falso: f_p é primo se, e somente se, p é primo? Justifique.

138. Se $2 \mid f_n$, prove que $4 \mid (f_{n+1}^2 - f_{n-1}^2)$.

Resolução: Observemos que:

$$f_{n+1}^2 - f_{n-1}^2 = (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1})$$

Mas $f_{n+1} - f_{n-1} = f_n$ e $f_{n+1} + f_{n-1} = f_n + f_{n-1} + f_{n-1} = f_n + 2f_{n-1}$.

Logo: $f_{n+1}^2 - f_{n-1}^2 = f_n(f_n + 2f_{n-1}) = f_n^2 + 2f_nf_{n-1}$. Como $2 \mid f_n$, então $4 \mid f_n^2$ e $4 \mid 2f_n$. Donde $4 \mid (f_{n+1}^2 - f_{n-1}^2)$.

139. Se $3 \mid f_n$, prove que $9 \mid (f_{n+1}^3 - f_{n-1}^3)$.

140. Prove que $2 \mid (f_{n+3} - f_n)$, $\forall n \geqslant 1$.
Conclua então que $f_3, f_6, f_9, \ldots$ são todos números pares.

Resolução: Como

$$f_{n+3} - f_n = f_{n+1} + f_{n+2} - f_n = f_{n+1} + f_{n+1} + f_n - f_n = 2f_{n+1}$$

então $2 \mid (f_{n+3} - f_n)$, $\forall n \geqslant 1$. Em particular: $f_6 - f_3 = 2f_4$ e como $f_3 = 2$ e $f_4 = 3$, então $f_6 = 2 + 6$. De um modo geral, sempre que f_n é par a fórmula $f_{n+3} = f_n + 2f_{n+1}$ garante que f_{n+3} também é par, o que conclui a justificativa.

141. Prove que $5 \mid (f_{n+5} - 3f_n)$, $\forall n \geqslant 1$. Conclua a partir daí que $f_5, f_{10}, f_{15}, \ldots$ são múltiplos de 5.

142. Se $\text{mdc}(m, n) = 1$, prove que $f_mf_n \mid f_{mn}$.

143. Há uma conjectura segundo a qual somente cinco números de Fibonacci são números triangulares. Ache-os.

APÊNDICE I

AXIOMAS DE PEANO

1. Introdução

Numa teoria matemática, quando há necessidade de definir algo, isso obviamente é feito em termos de conceitos anteriores. Mas estes, por sua vez, também dependem de idéias precedentes. E assim por diante. Como evitar então que esse processo leve a círculos viciosos ou ao chamado *regressus in infinitum*?

Para o método axiomático a resposta consta de duas partes: primeiro, simplesmente aceitar certos termos da teoria sem uma explicação formal de seu significado — estes termos são chamados *conceitos primitivos* (na geometria elementar, por exemplo, em geral ponto, reta e plano); além disso, introduzir alguns *axiomas*, ou seja, certas proposições que se tomam como verdadeiras independentemente de qualquer demonstração. Na teoria então só há mais uma classe de proposições: a daquelas que se demonstram a partir dos axiomas por raciocínios lógicos corretos.

2. Os axiomas

Com vistas à fundamentação lógica da Aritmética, Peano escolheu três conceitos primitivos: o *zero*, o *número natural* e a relação *é sucessor de*. E, para caracterizá-los, formulou os seguintes axiomas:

$\mathbf{P}_1$ Zero é um número natural.

$\mathbf{P}_2$ Se a é um número natural, então a tem um único sucessor que também é um número natural.

$\mathbf{P}_3$ Zero não é sucessor de nenhum número natural.

$\mathbf{P}_4$ Dois números naturais que têm sucessores iguais são, eles próprios, iguais.

$\mathbf{P}_5$ Se uma coleção S de números naturais contém o zero e, também, o sucessor de todo elemento de S, então S é o conjunto de todos os números naturais.

Adotaremos as seguintes notações: 0 para indicar o zero, a^+ para indicar o sucessor de um número natural a e $\mathbb{N}$ para denotar o conjunto dos números naturais. Isto posto, os axiomas de Peano podem assim ser enunciados:

$\mathbf{P}_1$ $0 \in \mathbb{N}$

$\mathbf{P}_2$ $a \in \mathbb{N} \Rightarrow a^+ \in \mathbb{N}$

$\mathbf{P}_3$ $(\forall a)(a \in \mathbb{N} \Rightarrow a^+ \neq 0)$

$\mathbf{P}_4$ $a^+ = b^+ \Rightarrow a = b$

$\mathbf{P}_5$ Se $S \subset \mathbb{N}$ e (i) $0 \in S$, (ii) $a \in S \Rightarrow a^+ \in S$, então $S = \mathbb{N}$.

O axioma $\mathbf{P}_1$ garante que $\mathbb{N} \neq \varnothing$. Em $\mathbf{P}_2$ deve-se subentender a unicidade de a^+. Do axioma $\mathbf{P}_4$ decorre que: $a \neq b \Rightarrow a^+ \neq b^+$, o que é óbvio pois $a^+ = b^+$ implica $a = b$. O axioma $\mathbf{P}_5$ chama-se *axioma da indução completa*.

PROPOSIÇÃO 1 Se $a \in \mathbb{N}$, então $a^+ \neq a$.

Demonstração: Seja $S = \{a \in \mathbb{N} \mid a^+ \neq a\}$. O axioma $\mathbf{P}_3$ garante que $0 \in S$. Se $a \in S$, então $a^+ \neq a$ e, pela observação anterior, $(a^+)^+ \neq a^+$. Logo $a^+ \in S$, sempre que $a \in S$. Por $\mathbf{P}_5$ conclui-se que $S = \mathbb{N}$. Ou seja: para todo $a \in \mathbb{N}$, $a^+ \neq a$. ■

PROPOSIÇÃO 2 Se $b \in \mathbb{N}$, $b \neq 0$, então existe $a \in \mathbb{N}$ tal que $a^+ = b$.

Demonstração: Seja $S = \{0\} \cup \{y \in \mathbb{N} \mid y \neq 0 \text{ e } x^+ = y$, para algum $x \in \mathbb{N}\}$. Por construção $0 \in S$. Obviamente $0^+ \in S$. Agora, se $a \in S$ e $a \neq 0$, então $a = b^+$, para algum $b \in \mathbb{N}$. Daí $a^+ = (b^+)^+$ e portanto $a^+ \in S$. Novamente o axioma $\mathbf{P}_5$ garante que $S = \mathbb{N}$ e portanto a proposição é verdadeira. ■

PROPOSIÇÃO 3 (primeiro princípio de indução completa): Suponhamos que a todo número natural n esteja associada uma afirmação P(n) tal que:

i P(0) é verdadeira.

ii $P(r^+)$ é verdadeira, sempre que P(r) é verdadeira.

Então P(n) é verdadeira para todo $n \in \mathbb{N}$.

Demonstração: Basta verificar que $S = \{n \in \mathbb{N} \mid P(n) \text{ é verdadeira}\}$ satisfaz as hipóteses do axioma $\mathbf{P}_5$, o que, aliás, é imediato. ■

3. Adição em $\mathbb{N}$

A adição $(x, y) \rightarrow x + y$ em $\mathbb{N}$ é definida mediante as seguintes condições:

- $a + 0 = a$
- $a + b^+ = (a + b)^+$

Em $a + b = c$, a e b são as *parcelas* e c a *soma*. Como não poderia deixar de ser, adotaremos as seguintes notações: $0^+ = 1$, $1^+ = 2$, $2^+ = 3$, ... Nessas condições obtemos, por exemplo

$$1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2$$
$$1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3$$
$$1 + 3 = 1 + 2^+ = (1 + 2)^+ = 3^+ = 4$$
$$r + 1 = r + 0^+ = (r + 0)^+ = r^+, \forall r \in \mathbb{N}.$$

3.1 Propriedades da adição

$\mathbf{a_1}$ *Associativa*: $a + (b + c) = (a + b) + c$, $\forall a, b, c \in \mathbb{N}$.

Prova (por indução sobre c):

$c = 0$: $a + (b + 0) = a + b = (a + b) + 0$

Vamos supor: $(a + b) + r = a + (b + r)$
Então: $(a + b) + r^+ = [(a + b) + r]^+ = [a + (b + r)]^+ =$
$= a + (b + r)^+ = a + (b + r^+)$. ■

$\mathbf{a_2}$ *Comutativa*: $a + b = b + a$, $\forall a, b \in \mathbb{N}$ (Exercício)

$\mathbf{a_3}$ O zero é o *elemento neutro* da adição.

A definição de adição e $\mathbf{a_2}$ garantem que 0 é elemento neutro. Deixamos como exercício a demonstração de que só há um elemento neutro para a adição.

$\mathbf{a_4}$ *Lei do cancelamento da adição*: $a + b = a + c \Rightarrow b = c$

Prova (indução sobre a):

$a = 0 \Rightarrow b = a + b = a + c = c$

Façamos a hipótese: $r + b = r + c \Rightarrow b = c$
Suponhamos agora $r^+ + b = r^+ + c$. Então:

$$(b + r)^+ = b + r^+ = c + r^+ = (c + r)^+$$

Então, devido a $\mathbf{P_4}$: $b + r = c + r$. Donde $b = c$. ■

Na seqüência precisaremos do seguinte resultado:

- $a + b = 0 \Rightarrow a = b = 0$

Vamos supor $b \neq 0$. Então $b = u^+$, para algum $u \in \mathbb{N}$. Daí

$$0 = a + b = a + u^+ = (a + u)^+$$

o que é absurdo. Assim $b = 0$ e então $a = 0$. ■

4. Multiplicação em $\mathbb{N}$

A multiplicação $(x, y) \rightarrow xy$ (ou $x \cdot y$) de números naturais é definida pelas condições seguintes:

- $a \cdot 0 = 0$
- $a \cdot b^+ = ab + a$

Numa igualdade $ab = c$, a e b são os *fatores* e c o *produto*. Observemos os seguintes exemplos:

$$1 \cdot 1 = 1 \cdot 0^+ = 1 \cdot 0 + 1 = 0 + 1 = 1$$
$$1 \cdot 2 = 1 \cdot 1^+ = 1 \cdot 1 + 1 = 1 + 1 = 2$$
$$2 \cdot 1 = 2 \cdot 0^+ = 2 \cdot 0 + 2 = 0 + 2 = 2$$
$$2 \cdot 2 = 2 \cdot 1^+ = 2 \cdot 1 + 2 = 2 + 2 = 4$$

4.1 Propriedades da multiplicação

Mostremos primeiro que $0 \cdot a = 0$, para todo $a \in \mathbb{N}$. Para $a = 0$ esse resultado decorre diretamente da definição dada. Supondo $0 \cdot r = 0$, então $0 \cdot r^+ = 0 \cdot r + 0 = 0 + 0 = 0$.

Também é fácil provar, por indução, que $1 \cdot a = a$, para todo $a \in \mathbb{N}$.

Com isso torna-se possível demonstrar

$\mathbf{m_7}$ $(a + b)c = ac + bc$ e $a(b + c) = ab + ac$, $\forall a, b, c \in \mathbb{N}$ (propriedade *distributiva* da multiplicação em relação à adição).

Prova (primeira condição — indução sobre c):

$$c = 0: (a + b) \cdot 0 = 0 = 0 + 0 = a \cdot 0 + b \cdot 0$$

Vamos supor $(a + b)r = ar + br$.
Então: $(a + b)r^+ = (a + b)r + (a + b) = (ar + br) +$
$+ (a + b) = (ar + a) + (br + b) = ar^+ + br^+$ ■

Fica como exercício a prova de que $a(b + c) = ab + ac$ (usar indução sobre a).

Deixamos de provar as propriedades $\mathbf{m}_1$, $\mathbf{m}_2$ e $\mathbf{m}_3$ enunciadas no corpo do capítulo, item 2.2. Sugerimos ao leitor tentar demonstrá-las.

$\mathbf{m}_4$ $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (*lei do anulamento do produto*)

Vamos supor $b \neq 0$, o que implica $b = r^+$, $r \in \mathbb{N}$. Então:

$$0 = ab = ar^+ = ar + a$$

Daí, como já vimos, $ar = a = 0$. ■

As propriedades $\mathbf{m}_5$ e $\mathbf{m}_6$ serão focalizadas no próximo item.

5. Relação de ordem em $\mathbb{N}$

Já definimos, no item 2.3 (capítulo II), a relação $\leqslant$ (menor que ou igual) em $\mathbb{N}$. Lembremos que $a \leqslant b$ significa $b = a + u$, para algum $u \in \mathbb{N}$. Se $b = a + v$, $v \neq 0$, então se anota $a < b$ (a é menor que b). As relações $\geqslant$ (maior que ou igual) e $>$ (maior que) são definidas, respectivamente, pelas equivalências: "$x \geqslant y \iff y \leqslant x$" e "$x > y \iff y < x$".

5.1 Propriedades da relação de ordem

$\mathbf{O}_1$ $a \leqslant a$, $\forall a \in \mathbb{N}$ (*reflexiva*)

Prova: $a = a + 0$ ■

$\mathbf{O}_2$ $a \leqslant b$ e $b \leqslant a \Rightarrow a = b$ (*anti-simétrica*)

Prova: Por hipótese $b = a + u$ e $a = b + v$ $(u, v \in \mathbb{N})$. Donde $a = a + (u + v)$ e, pela lei do cancelamento da adição, $u + v = 0$. Daí $u = v = 0$, como já provamos, e portanto $a = b$. ■

$\mathbf{O}_3$ $a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$ (*transitiva*)

Exercício

$\mathbf{O}_4$ Para quaisquer $a, b \in \mathbb{N}$, $a \leqslant b$ ou $b \leqslant a$.

Prova: Para cada $b \in \mathbb{N}$ seja S_b o subconjunto de $\mathbb{N}$ formado pelos elementos n para os quais se verifica ao menos uma das seguintes condições: (a) existe $u \in \mathbb{N}$ tal que $b = n + u$; (b) existe $v \in \mathbb{N}$ tal que $n = b + v$. Como para $n = 0$ a sentença (a) se verifica com $u = b$, então $0 \in S_b$. Seja $r \in S_b$. Se $r = b$, então $r^+ = b^+ = b + 1$ e portanto $r^+ \in S_b$, já que verifica (b). Suponhamos agora $b = r + u$, $u \neq 0$; então $u = v^+ = v + 1$, para algum $v \in \mathbb{N}$, e daí $b = r + (v + 1) = r^+ + v$, ou seja, r^+ satisfaz (a) e portanto pertence a S_b. Finalmente, se $r = b + v$, $v \neq 0$, então $r^+ = (b + v)^+ = b + v^+$, o que significa que $r^+ \in S_b$, pois cumpre a condição (b).

Donde $S_b = \mathbb{N}$ e, por isso, para todo $b \in \mathbb{N}$, qualquer que seja o número natural a, ou $b = a + u$ ou $a = b + v$. Ou seja: $a \leqslant b$ ou $b \leqslant a$. ■

$\mathbf{O}_5$ $a \leqslant b \Rightarrow a + c \leqslant b + c$, $\forall c \in \mathbb{N}$ (*compatibilidade com a adição*)

Exercício

$\mathbf{O}_6$ $a \leqslant b \Rightarrow ac \leqslant bc$, $\forall c \in \mathbb{N}$ (*compatibilidade com a multiplicação*)

Prova: Por hipótese $b = a + u$, para algum $u \in \mathbb{N}$. Donde $bc = (a + u)c = ac + uc$, do que resulta $ac \leqslant bc$. ■

$\mathbf{O}_7$ $a < b \Rightarrow a + 1 \leqslant b$ (já provada no corpo deste capítulo — item 2)

$\mathbf{O}_8$ *Princípio do menor número natural.* Qualquer que seja o subconjunto não vazio $S \subset \mathbb{N}$, S possui mínimo.

Prova: Seja $H = \{n \in \mathbb{N} \mid n \leqslant x, \ \forall x \in S\}$. Como $0 \leqslant a$, $\forall a \in S$ $(a = 0 + a)$, então $0 \in H$. Tomemos $a \in S$, o que é possível pois $S \neq \emptyset$. Observando que $a < a + 1$, pode-se afirmar que $a + 1 \notin H$ (se pertencesse, deveria ocorrer $a + 1 \leqslant a$) e portanto $H \neq \mathbb{N}$. Levando em conta $\mathbf{P}_5$, necessariamente existe um elemento $b \in \mathbb{N}$ tal que $b \in H$ e $b + 1 \notin H$ (caso contrário se teria $H = \mathbb{N}$). Mostremos que $b = \min S$. De fato:

- Como $b \in H$, então $b \leqslant x$, $\forall x \in S$.
- Vamos supor que $b \notin S$. Então $b < x$, para todo $x \in S$, e daí $b + 1 \leqslant x$, também para todo $x \in S$, o que implica $b + 1 \in H$. Mas isto é impossível. Esta contradição nos leva a concluir que $b \in S$. ■

Uma pergunta que cabe perfeitamente após a construção axiomática que fizemos de $\mathbb{N}$ é a seguinte: Será que a seqüência formada pelo zero e seus sucessores esgota realmente o conjunto dos números naturais? Será que não pode ocorrer

$$a < r < a^+ = a + 1$$

para algum par de elementos $a, r \in \mathbb{N}$? Mostraremos que não.

Supondo $a < r < a + 1$, então $r = a + u$ $(u \neq 0)$ e $a + 1 = r + v$ $(v \neq 0)$. Portanto

$$a + 1 = a + (u + v)$$

o que implica $u + v = 1$. Considerando que $u \neq 0$, então (proposição 2) $u = r^+ = r + 1$. Assim chegamos a

$$1 = u + v = (r + 1) + v = (r + v) + 1$$

e, portanto, $r + v = 0$. Mas daí decorre, conforme provamos no item 3.1, que $r = v = 0$. Absurdo. Assim, efetivamente, para todo $a \in \mathbb{N}$:

$$\{x \in \mathbb{N} \mid a < x < a + 1\} = \emptyset$$

5.2 Lei da tricotomia em $\mathbb{N}$

Para quaisquer $a, b \in \mathbb{N}$ vale uma e uma só das relações: $a = b$, $a < b$ ou $a > b$. De fato, por $\mathbf{O_4}$: $a \leqslant b$ ou $a \geqslant b$. Então $b = a + u$ ou $a = b + v$. Supondo $a \neq b$, devemos ter $u \neq 0$ para a primeira possibilidade e $v \neq 0$ para a segunda. Ou seja: $a \neq b \Rightarrow a < b$ ou $b < a$. Se ocorressem simultaneamente $a < b$ e $b < a$, então $b = a + r$ $(r \neq 0)$ e $a = b + s$ $(s \neq 0)$. Daí $a = a + (r + s)$. Então $r + s = 0$ e portanto $r = s = 0$. Absurdo. Assim, se $a, b \in \mathbb{N}$, então $a = b$, $a < b$ ou $a > b$, exclusivamente. Esta é chamada *lei da tricotomia* em $\mathbb{N}$.

Provemos a partir dessa observação a propriedade $\mathbf{m_5}$: $ab = ac$, $a \neq 0 \Rightarrow b = c$.

Se $b < c$, então $c = b + v$ $(v \neq 0)$. Logo $ab = ac = ab + av$, o que implica $av = 0$. Donde, por $\mathbf{m_4}$, $a = 0$ ou $v = 0$, o que é absurdo. Da mesma forma não pode ocorrer $c < b$.

Vejamos agora como se pode provar $\mathbf{m_6}$: $ab = 1 \Rightarrow a = b = 1$.

Da hipótese decorre que $a \neq 0$ e $b \neq 0$. Logo $a \geqslant 1$ e $b \geqslant 1$. Supondo, por exemplo, $a > 1$, então $a = 1 + v$ $(v \neq 0)$. Como $b = 1 + u$ (pois $b \geqslant 1$), podemos concluir que

$$1 = ab = (1 + v)(1 + u) = 1 + u + v + uv$$

o que leva a

$$v + (u + uv) = 0$$

e daí $u + uv = v = 0$, o que não é possível. Donde $a = 1$ e então $b = 1$.

EXERCÍCIOS

144. Se a e b são números naturais e $a + b = 1$, prove que $a = 1$ ou $b = 1$.

145. Sejam a e b números naturais não nulos. Prove que $a \leqslant ab$ e $b \leqslant ab$.

Resolução: Seja $c = ab$. Como $b \neq 0$, então $b \geqslant 1$ e portanto $b = 1 + u$ $(u \in \mathbb{N})$. Então $c = ab = a(1 + u) = a + au$, do que resulta $a \leqslant c$.

146. Se a e b são números naturais e se $ab = 3$, prove que $a = 1$ ou $b = 1$.

147. Se a e b são números naturais não nulos e se $a + b = 2$, prove que $a = b = 1$.

148. Se $a + b = 3$, onde a e b são números naturais, não nulos, prove que $a = 1$ ou $b = 1$.

149. Se $ac < bc$ e $c \neq 0$, prove que $a < b$.

Resolução: Vamos supor $a \geqslant b$, o que se traduz por $a = b + u$, para algum $u \in \mathbb{N}$. Então $ac = (b + u)c = bc + uc$. Donde $bc \leqslant ac$, o que contraria a hipótese.

150. Se $a + c < b + c$, prove que $a < b$.

151. Se $a \leqslant b$, prove que: $c < b - a \iff c + a < b$.

152. Se $a < b$, prove que: $a^n < b^n$, para todo $n \geqslant 1$.

Sugestão: Use indução sobre n e lembre que, por definição, $a^0 = 1$ e $a^{n+1} = a^n \cdot a$ $(n \geqslant 0;\ a \neq 0)$.

153. Prove que para todo $n \geqslant 1$, $n = 1 + 1 + \ldots + 1$ (n parcelas).

CAPÍTULO III

OS NÚMEROS INTEIROS

1. Números negativos: origens

Os algarismos que usamos hoje em dia surgiram na Índia, no século VII, e sua difusão pelo mundo se deve, em grande parte, aos árabes. Daí a designação "indo-arábicos" atribuída a eles. A maneira de grafar esses símbolos foi se modificando ao longo do tempo, e a forma moderna mal se assemelha à original. Importa, porém, que foi a partir da Índia, quando o Ocidente estava mergulhado na estagnação e no obscurantismo da primeira fase do período medieval, que o sistema de numeração posicional decimal começou a se tornar padrão. Inclusive o zero, que mesmo entre os gregos do período alexandrino era usado apenas para indicar "ausência" (o que já era um avanço em relação a outras épocas e outros povos), com os hindus ganhou "status" pleno de número.

Coube também aos hindus a introdução na matemática dos números negativos. O objetivo era indicar débitos. O primeiro registro do uso de números negativos de que se tem notícia foi feito pelo matemático e astrônomo hindu Brahmagupta (598-?), que já conhecia inclusive as regras para as quatro operações com números negativos. Bhaskara (séc.XII), outro matemático e astrônomo hindu, assinalou que todo número positivo tem duas raízes quadradas, uma negativa e outra positiva, e salientou também a impossibilidade de se extrair a raiz quadrada de um número negativo.

Ao introduzirem os números negativos, os hindus não tinham nenhuma preocupação de ordem teórica. Na verdade, os progressos matemáticos verificados na Índia, por essa época, ocorreram quase que por acaso e em boa parte devido ao descompromisso com o rigor e a formalidade.

Mas a aceitação e o entendimento pleno dos números negativos foi um processo longo. Basta ver algumas designações que receberam: Stifel (1486-1567) os chamava de números absurdos; Cardano (1501-1576), de números fictícios. Descartes (1596-1650) chamava de falsas as raízes negativas de uma equação. Outros, como F. Viete (1540-1603), importante matemático francês, simplesmente rejeitavam os números negativos.

2. Os inteiros

No capítulo II vimos que em $\mathbb{N}$ a diferença $a - b$ entre dois números a e b só está definida quando $a \geqslant b$. Assim, para fazer frente a todas as questões envolvendo números naturais e que levam à idéia de subtração, cumpre dar sentido a todas as expressões $a - b$, onde $a, b \in \mathbb{N}$, através de uma ampliação conveniente de $\mathbb{N}$.

Num enfoque informal, os novos números, correspondentes às diferenças $a - b$ $(a < b)$, são interpretados intuitivamente (como débitos, por exemplo) e agregados a $\mathbb{N}$. Como resultado dessa união surge o conjunto dos números inteiros. Como é lícito admitir que se deva ter $0 - 1 = 1 - 2 = 2 - 3 = \ldots$, podemos indicar cada uma dessas diferenças por -1. De modo análogo surgem $-2, -3, -4, \ldots$. E se, por uma questão de uniformidade, passarmos a escrever $1 = +1$, $2 = +2$, ..., o conjunto dos números inteiros, que será indicado por $\mathbb{Z}$, é:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\}$$

Mas isso não basta; a seguir é preciso estender adequadamente a $\mathbb{Z}$ as operações e a relação de ordem de $\mathbb{N}$, o que é bem conhecido no plano elementar. Neste contexto, além de se ter $\mathbb{N} \subset \mathbb{Z}$, a subtração em $\mathbb{Z}$ sempre é possível, coerentemente com a de $\mathbb{N}$.

A construção formal de $\mathbb{Z}$ será feita no Apêndice II, ao fim deste capítulo.

3. Operações e relação de ordem em $\mathbb{Z}$

A adição e a multiplicação em $\mathbb{Z}$ serão definidas no já citado Apêndice III. Aqui nos limitaremos a citar suas propriedades fundamentais com vistas a ter uma estruturação inicial do assunto.

3.1 Adição em $\mathbb{Z}$

a_1 $(a + b) + c = a + (b + c)$, $\forall a, b, c \in \mathbb{Z}$ (associativa)
a_2 $a + b = b + a$, $\forall a, b \in \mathbb{Z}$ (comutativa)
a_3 $a + 0 = a$, $\forall a \in \mathbb{Z}$ (0 é o elemento neutro da adição)
a_4 Para todo $a \in \mathbb{Z}$, existe $b \in \mathbb{Z}$ de modo que $a + b = 0$.

Este elemento b, que é único, chama-se *oposto* de a e é indicado por $-a$.

Por exemplo, $-(+3) = -3$ e $-(-3) = +3$ pois $(-3) + (+3) = 0$. Em geral $-(-a) = a$ pois $a + (-a) = 0$. Como $0 + 0 = 0$, então $-0 = 0$.

PROPOSIÇÃO 1 Para quaisquer a, b, c $\in \mathbb{Z}$, se $a + c = b + c$, então $a = b$ (lei do cancelamento da adição).

Demonstração: $a + c = b + c \Rightarrow (a + c) + (-c) = (b + c) + (-c) \Rightarrow$
$\Rightarrow a + [c + (-c)] = b + [c + (-c)] \Rightarrow a + 0 = b + 0 \Rightarrow a = b$. ■

Dados quaisquer a, b $\in \mathbb{Z}$, chama-se *diferença* entre a e b e indica-se por $a - b$ o seguinte elemento de $\mathbb{Z}$: $a - b = a + (-b)$.

Como $(-b) \in \mathbb{Z}$, para todo $b \in \mathbb{Z}$, então a correspondência $(a, b) \to a - b$ é uma operação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ à qual denominamos *subtração* de números inteiros.

Observemos o seguinte:

- Para quaisquer a, b $\in \mathbb{Z}$

$$(a + b) + [(-a) + (-b)] = [a + (-a)] + [b + (-b)] = 0 + 0 = 0.$$

Logo $(-a) + (-b)$ é o oposto de $a + b$, o que se traduz por:

$$-(a + b) = (-a) + (-b)$$

Como podemos escrever simplesmente $(-a) + (-b) = -a - b$, então:

$$-(a + b) = -a - b$$

- Se a, b $\in \mathbb{Z}$

$$(a - b) + b = [a + (-b)] + b = a + [(-b) + b] = a + 0 = a$$

- Consideremos a equação $a + x = b$ $(a, b \in \mathbb{Z})$. Então:

$a + x = b \iff (-a) + (a + x) = (-a) + b \iff [(-a) + a] + x = (-a) + b \iff x = b - a$.

Logo, $b - a$ é a solução (única) de $a + x = b$ $(a, b \in \mathbb{Z})$. Como já vimos $b - a \in \mathbb{Z}$.

3.2 Multiplicação em $\mathbb{Z}$

m_1 $(ab)c = a(bc)$, $\forall a, b, c \in \mathbb{Z}$ (associativa)

m_2 $ab = ba$, $\forall a, b \in \mathbb{Z}$ (comutativa)

m_3 $a \cdot 1 = a$, $\forall a \in \mathbb{Z}$ (1 é o elemento neutro da multiplicação)

m_4 $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (lei do anulamento do produto)

d $a(b + c) = ab + ac$, $\forall a, b, c \in \mathbb{Z}$ (a multiplicação é distributiva em relação à adição)

Nota: A propriedade m_4 não é independente das demais. Ou seja, pode ser provada a partir das outras (incluindo as da adição), o que será feito no Apêndice II.

PROPOSIÇÃO 2 Se a, b, c $\in$ Z, então:

i $a(b - c) = ab - ac$ e $(a - b)c = ac - bc$

ii $a \cdot 0 = 0$ (logo $0 \cdot a = 0$)

iii $a(-b) = (-a)b = -(ab)$

iv $(-a)(-b) = ab$

v $(ab = ac$ e $c \neq 0) \Rightarrow b = c$ (lei do cancelamento da multiplicação)

Demonstração:

i Como

$$a(b - c) + ac = a[(b - c) + c] = ab$$

então:

$$a(b - c) = ab - ac$$

A demonstração da outra parte é análoga:

ii $a \cdot 0 = a \cdot (0 - 0) = a \cdot 0 - a \cdot 0 = 0$

iii $a(-b) = a[0 + (-b)] = a(0 - b) = a \cdot 0 - (ab) = 0 - (ab) = -(ab)$.
Ademais: $(-a)b = (0 - a)b = 0 \cdot b - (ab) = 0 - (ab) = -(ab)$

iv $(-a)(-b) = -[a(-b)]$, em virtude de **iii**. Mas, também por **iii**, $a(-b) = -(ab)$. Logo $(-a)(-b) = -[-(ab)] = ab$

v $ab = ac \Rightarrow ab + [-(ac)] = ac + [-(ac)] \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \xrightarrow{(a \neq 0)} b - c = 0 \Rightarrow b = c$. ■

3.3 Relação de ordem em $\mathbb{Z}$

Os elementos de $\mathbb{Z}_+ = \{0, +1, +2, \ldots\} = \mathbb{N}$ são chamados *inteiros positivos* e os de $\mathbb{Z}_+^* = \mathbb{Z}_+ - \{0\}$ *inteiros estritamente positivos*. Se a, b $\in \mathbb{Z}$, diz-se que a *é menor que ou igual a* b, e escrevemos $a \leqslant b$, se $b - a$ é positivo, isto é, se $b - a \in \mathbb{Z}_+$; e se $b - a$ é estritamente positivo, ou seja, se $b - a \in \mathbb{Z}_+^*$, então se diz que a *é menor que* b (notação $a < b$).

Quando $a \leqslant b$ pode-se escrever, alternativamente, que $b \geqslant a$ e dizer que b *é maior que ou igual a* a; e para $a < b$ a alternativa é $b > a$ (b *é maior que* a).

Os elementos de $\mathbb{Z}_- = \{0, -1, -2, \ldots\}$ se dizem *inteiros negativos* e os de $\mathbb{Z}_-^* = \{-1, -2, -3, \ldots\}$ *inteiros estritamente negativos*.

A seguir enunciaremos as propriedades mais importantes envolvendo as relações $\leqslant$ e $<$ sobre $\mathbb{Z}$. As seis primeiras são básicas e mostram que $\leqslant$ é uma relação de ordem total sobre $\mathbb{Z}$, compatível com a adição e a multiplica-

ção. (O leitor interessado encontrará mais detalhes sobre o assunto no Apêndice II.)

O$_1$ $a \leqslant a$ (reflexiva)

O$_2$ $a \leqslant b$ e $b \leqslant a \Rightarrow a = b$ (anti-simétrica)

O$_3$ $a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$ (transitiva)

O$_4$ $a \leqslant b$ ou $b \leqslant a$

As propriedades **O$_1$** a **O$_4$** garantem que $\leqslant$ é uma relação de ordem total sobre $\mathbb{Z}$. Delas decorre a *lei da tricotomia* em $\mathbb{Z}$: se $a, b \in \mathbb{Z}$, então $a = b$, $a < b$ ou $a > b$ (exclusivamente). A demonstração que foi feita para a lei correspondente em IN (Apêndice I; 5.2) é válida também no caso presente.

O$_5$ $a \leqslant b \Rightarrow a + c \leqslant b + c$, $\forall c \in \mathbb{Z}$ ($\leqslant$ é compatível com a adição)

O$_6$ $a \leqslant b$ e $0 \leqslant c \Rightarrow ac \leqslant bc$ ($\leqslant$ é compatível com a multiplicação)

Outras propriedades

- $a \leqslant b \Longleftrightarrow -b \leqslant -a \Longleftrightarrow 0 \leqslant b - a$
- $a < b \Longleftrightarrow -b < -a \Longleftrightarrow 0 < b - a$
- $a \leqslant b$ e $c \leqslant d \Rightarrow a + c \leqslant b + d$
- $a \leqslant b$ e $c < d \Rightarrow a + c < b + d$
- Regras de sinais: **i** $a > 0$ e $b > 0 \Rightarrow ab > 0$; **ii** $a < 0$ e $b < 0 \Rightarrow ab > 0$; **iii** $a < 0$ e $b > 0 \Rightarrow ab < 0$.

Provemos **ii**: De $a < 0$ e $b < 0$ resulta que $0 < -a$ e $0 < -b$; daí, por **i**, $0 < (-a)(-b)$. Mas $(-a)(-b) = ab$, como já vimos. Logo $0 < ab$.

- $a^2 \geqslant 0$ para todo $a \in \mathbb{Z}$ e $a^2 > 0$ sempre que $a \neq 0$.

De fato, se $a > 0$ ou $a < 0$, então a regra de sinais garante que $a^2 = a \cdot a > 0$; e, se $a = 0$, obviamente $a^2 = 0$.

- $a < b$ e $c > 0 \Rightarrow ac < bc$
- $a < b$ e $c < 0 \Rightarrow ac > bc$
- $ac \leqslant bc$ e $c > 0 \Rightarrow a \leqslant b$
- $ac \leqslant bc$ e $c < 0 \Rightarrow a \geqslant b$

Seja S um subconjunto não vazio de $\mathbb{Z}$. Todo elemento $k \in \mathbb{Z}$ tal que $k \leqslant x$, para todo $x \in S$, chama-se *cota inferior* de S. Uma cota inferior de S que pertença a S chama-se *mínimo* de S.

S não pode ter mais que um mínimo. Com efeito, se m e m' são mínimos de S, então $m \leqslant m'$ (pois m é mínimo de S e $m' \in S$) e $m' \leqslant m$ (pela inversão do raciocínio). Logo $m = m'$.

Usaremos a notação min S (ou min(S)) para indicar o mínimo de S, caso este exista.

O$_7$ *Princípio do menor inteiro*: Seja $S \neq \emptyset$ um subconjunto de $\mathbb{Z}$. Se S admite alguma cota inferior em $\mathbb{Z}$, então S possui mínimo.

A *demonstração* neste caso recai na do princípio do menor número natural. Vejamos como. Seja $S' = \{x - k \mid x \in S\}$, onde k é uma cota inferior de S que, por hipótese, existe. Notemos que $S' \neq \emptyset$ (pois $S \neq \emptyset$) e que, como $k \leqslant x$, então $x - k \geqslant 0$ para todo $x \in S$, ou seja, $S' \cup Z_+ = \mathbb{N}$. Logo, pelo princípio do menor número natural, S' tem um mínimo $m_0 = m - k$, para algum $m \in S$. Mostremos que $m = \min(S)$. Se $x \in S$, então $x - k \in S'$ e daí $m - k \leqslant x - k$. Donde $m \leqslant x$, e como $m \in S$, então efetivamente $m = \min(S)$.

O procedimento da demonstração pode ser visto no seguinte exemplo: Seja $S = \{-1, 0, 1, 2, 3, \ldots\}$. Neste caso, tomando $k = -2$ por exemplo, então $S' = \{x - k \mid x \in S\} = \{-1 - (-2), 0 - (-2), 1 - (-2), 2 - (-2), \ldots\} = \{1, 2, 3, 4, \ldots\}$ cujo mínimo é $1 = m - (-2)$. Daí $m = -1 = \min(S)$, o que, evidentemente, já poderíamos ter concluído de saída se o objetivo fosse apenas esse.

4. Indução

4.1 Primeiro princípio de indução

Seja a um número inteiro e suponhamos que a cada $n \geqslant a$ esteja associada uma afirmação $P_{(n)}$. Admitamos ainda que seja possível provar o seguinte:

i $P_{(a)}$ é verdadeira.

ii Para todo $r \geqslant a$, se $P_{(r)}$ é verdadeira, então $P_{(r+1)}$ também é verdadeira.

Nessas condições $P_{(n)}$ é verdadeira para todo $n \geqslant a$.

A demonstração da validade desse princípio não difere em nada daquela que foi feita do princípio análogo em IN (cap. II, 3.1). Daí não a fazermos aqui.

Exemplo 1: Provemos, usando o primeiro princípio de indução, que $2^{n+1} \geqslant n + 2$, para todo $n \geqslant -1$.

$$n = -1:\ 2^{(-1)+1} = 2^0 = 1 = (-1) + 2$$

Seja $r \geqslant -1$ e suponhamos $2^{r+1} \geqslant r + 2$ (hipótese de indução).

$$n = r + 1:\ 2^{(r+1)+1} = 2^{r+1} \cdot 2 \geqslant (r + 2) \cdot 2$$

(pela hipótese de indução). Mas $(r + 2) \cdot 2 = 2r + 4 = (r + 3) + (r + 1) \geqslant r + 3$, visto que, sendo $r \geqslant -1$, então $r + 1 \geqslant 0$. Assim:

$2^{(r+1)+1} \geqslant r + 3 = (r + 1) + 2.$

4.2 Segundo princípio de indução

Seja $P_{(n)}$ uma afirmação associada a todo n maior que ou igual a um certo $a \in \mathbb{Z}$, dado *a priori*. Suponhamos que seja possível provar as duas condições a seguir:

i $P_{(a)}$ é verdadeira.

ii Para todo $r > a$, se $P_{(k)}$ é verdadeira sempre que $a \leqslant k < r$, então $P_{(r)}$ também é verdadeira.

Então $P_{(n)}$ é verdadeira para qualquer $n \geqslant a$.

Prova: Seja $S = \{m \in \mathbb{Z} \mid m \geqslant a \text{ e } P_{(m)} \text{ é falsa}\}$. Devemos provar que $S = \varnothing$. Admitamos que se pudesse ter $S \neq \varnothing$ e seja, segundo $\mathbf{O_7}$, $m_0 = \min(S)$. Como $P_{(a)}$ é verdadeira, devido à hipótese **i**, então $m_0 > a$. Logo, para todo $k \in \mathbb{Z}$, $a \leqslant k < m_0$, $P_{(k)}$ é verdadeira (pois m_0 é o mínimo dos $m \geqslant a$ para os quais $P_{(m)}$ é falsa). Donde, pela hipótese **ii**, $P(m_0)$ também é verdadeira, o que é absurdo.

Assim, efetivamente $S = \varnothing$ e $P_{(m)}$ é verdadeira para todo $m \geqslant a$. ■

4.3 Somatórios e produtórios em $\mathbb{Z}$

A adição e a multiplicação em $\mathbb{Z}$ podem ser estendidas para n parcelas e n fatores ($n \geqslant 2$), respectivamente, por recorrência, tal como foi feito em $\mathbb{N}$: se $a_1, a_2, \ldots, a_n \in \mathbb{Z}$,

$$a_1 + a_2 + \ldots + a_n = (a_1 + a_2 + \ldots + a_{n-1}) + a_n$$

e

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n$$

Também não há motivos para mudar as notações:

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i$$

$$a_1 a_2 \ldots a_n = \prod_{i=1}^{n} a_i$$

O índice i usado poderia ser substituído por qualquer outra letra (o "a" não seria conveniente). Se $n = 1$, faz-se:

$$\sum_{i=1}^{n} a_i = a_1 \qquad \text{e} \qquad \prod_{i=1}^{n} a_i = a_1$$

Com isso, e usando indução, é possível generalizar várias propriedades vistas em Operações e relação de ordem em $\mathbb{Z}$ (item 3). Para tanto são peças fundamentais as identidades

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n \quad \text{e} \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n \qquad (n \geqslant 2)$$

que simplesmente expressam os conceitos introduzidos neste item com a notação mais conveniente.

- Se $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ $(n \geqslant 1)$, então

$$b\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} b a_i$$

De fato:

$$n = 1: \; b\left(\sum_{i=1}^{n} a_i\right) = b a_1 = \sum_{i=1}^{n} b a_i$$

Seja $r \geqslant 1$ e suponhamos

$$b\left(\sum_{i=1}^{r} a_i\right) = \sum_{i=1}^{r} b a_i$$

$n = r + 1$:

$$b\left(\sum_{i=1}^{r+1} a_i\right) = b\left(\sum_{i=1}^{r} a_i + a_{r+1}\right) =$$

$$= b\left(\sum_{i=1}^{r} a_i\right) + b a_{r+1} = \sum_{i=1}^{r} b a_i + b a_{r+1} = \sum_{i=1}^{r+1} b a_i$$

Esta é uma generalização da propriedade distributiva da multiplicação em relação à adição (**d**; 3.2).

- Tudo que de geral foi visto no capítulo II (3.2) sobre somatórios e produtórios de números naturais também vale quando estes são substituídos por inteiros quaisquer. O motivo, obviamente, é que as propriedades em que aqueles resultados se apóiam tanto valem em $\mathbb{N}$ como em $\mathbb{Z}$. **Por exemplo**

$$\sum_{i=1}^{n} a = na \quad \text{e} \quad \prod_{i=1}^{n} a = a^n, \text{ para todo } a \in \mathbb{Z}$$

Assim

$$\sum_{i=1}^{5} (-3) = 5(-3) = -15 \quad \text{e} \quad \prod_{i=1}^{5} (-3) = (-3)^5 = -243$$

- A propriedade "$a \leqslant b$ e $c \leqslant d \Rightarrow a + c \leqslant b + d$" pode ser assim generalizada: se $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ ($n \geqslant 1$) e $a_i \leqslant b_i$ ($i = 1, 2, \ldots, n$), então:

$$\sum_{i=1}^{n} a_i \leqslant \sum_{i=1}^{n} b_i$$

De fato:

$$n = 1: \quad \sum_{i=1}^{n} a_i = a_1 \leqslant b_1 = \sum_{i=1}^{n} b_i$$

Se $r \geqslant 1$, suponhamos $\sum_{i=1}^{r} a_i \leqslant \sum_{i=1}^{r} b_i$

$n = r + 1$:

$$\sum_{i=1}^{r+1} a_i = \sum_{i=1}^{r} a_i + a_{r+1} \leqslant \sum_{i=1}^{r} b_i + b_{r+1} = \sum_{i=1}^{r+1} b_i$$

A versão mais comum dessa propriedade é que n desigualdades $a_i \leqslant b_i$ ($i = 1, 2, \ldots, n$) podem ser "somadas membro a membro".

- A generalização da propriedade "$a \leqslant b$ e $c < d \Rightarrow a + c < b + d$" é a seguinte:

Se nas n desigualdades $a_i \leqslant b_i$ ($i = 1, 2, \ldots, n$; $n \geqslant 1$) para uma delas pelo menos se verificar $a_k < b_k$, então:

$$\sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i$$

- Usemos o resultado anterior para mostrar que se $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ ($n \geqslant 1$), então:

$$\sum_{i=1}^{n} a_i^2 = 0 \iff a_i = 0 \ (i = 1, 2, \ldots, n)$$

Se cada $a_i = 0$, obviamente $\sum_{i=1}^{n} a_i^2 = 0$.

Para a recíproca vamos levar em conta que $0 \leqslant a_1^2, 0 \leqslant a_2^2, \ldots, 0 \leqslant a_n^2$, resultado já exposto em 3. Se, para um certo índice k, ocorresse $0 < a_k^2$, então, levando em conta a propriedade anterior:

$$0 = \sum_{i=1}^{n} 0 < \sum_{i=1}^{n} a_i^2$$

o que contraria a hipótese. Logo $a_1^2 = a_2^2 = \ldots = a_n^2 = 0$ e, devido à lei do anulamento do produto: $a_1 = a_2 = \ldots = a_n = 0$.

5. Valor absoluto

DEFINIÇÃO 1 Para todo $a \in \mathbb{Z}$, o *valor absoluto* ou *módulo* de a (notação $|a|$) é definido pelas seguintes condições:

$|a| = a$ sempre que $a \geqslant 0$

$|a| = -a$ se $a < 0$

Por exemplo: $|-3| = -(-3) = +3$

PROPOSIÇÃO 3 Se a e b são elementos quaisquer de $\mathbb{Z}$, então:

i $|a| = |-a|$ **iii** $|ab| = |a|\,|b|$

ii $-|a| \leqslant a \leqslant |a|$ **iv** $|a + b| \leqslant |a| + |b|$

Demonstração: Quando $a = 0$ ou $b = 0$, as afirmações são imediatas. Portanto admitamos $a \neq 0$ e $b \neq 0$.

i Se $a > 0$, então $-a < 0$ e daí $|a| = a$ e $|-a| = -(-a) = a$. Se $a < 0$, então $|a| = -a$ e $|-a| = -a$, pois $-a > 0$.

ii Suponhamos $a > 0$ e portanto $-a < 0$; daí $-a < a$; como neste caso $-|a| = -a$ e $|a| = a$, então $-|a| = -a < a = |a|$. Para o caso $a < 0$, o procedimento é o mesmo.

iii Se $a > 0$ e $b > 0$, então $ab > 0$ e portanto $|ab| = ab = |a|\,|b|$. Se $a < 0$ e $b > 0$, então $|a| = -a$, $|b| = b$ e $|ab| = -(ab)$ pois $ab < 0$; como $|a|\,|b| = (-a)b = -(ab)$, então $|ab| = |a|\,|b|$. Se $a < 0$ e $b < 0$, então $ab > 0$ e portanto $|ab| = ab$, $|a| = -a$ e $|b| = -b$; e posto que $|a|\,|b| = (-a)(-b) = ab$, então $|ab| = |a|\,|b|$.

iv Devido a **ii** valem

$$-|a| \leqslant a \leqslant |a|$$
$$-|b| \leqslant b \leqslant |b|$$

Somando membro a membro essas desigualdades:

$$-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|$$

Se $|a + b| = a + b$, como $a + b \leqslant |a| + |b|$, então $|a + b| \leqslant |a| + |b|$. E se $|a + b| = -(a + b)$, então $-|a + b| = a + b$; como $-(|a| + |b|) \leqslant a + b$, então $-(|a| + |b|) \leqslant -|a + b|$; donde $|a + b| \leqslant |a| + |b|$. ■

Exemplo 2: Provemos que

$$|a| - |b| \leqslant |a - b| \leqslant |a| + |b|$$

para quaisquer $a, b \in \mathbb{Z}$.

Como $a = (a - b) + b$, a parte **iv** da proposição anterior nos garante que

$$|a| = |(a - b) + b| \leqslant |a - b| + |b|$$

e portanto $|a| - |b| \leqslant |a - b|$. Finalmente:

$$|a - b| = |a + (-b)| \leqslant |a| + |-b| = |a| + |b|.$$

EXERCÍCIOS

154. Seja $a \in \mathbb{Z}$, $a \neq 0$. Prove por indução que: i) $(-a)^n = a^n$, para todo $n \geqslant 0$ par; ii) $(-a)^n = -a^n$, para todo $n \geqslant 1$ ímpar.

155. Para todo $r \geqslant 0$, prove que:

a) $\sum_{i=1}^{2r} (-1)^i = 0$ b) $\sum_{i=1}^{2r+1} (-1)^i = -1$

156. Use indução para provar que:

a) $0 < a \Rightarrow 0 < a^n$, $\forall n \geqslant 0$

b) $a < 0 \Rightarrow 0 < a^{2n}$, $\forall n \geqslant 0$

c) $a < 0 \Rightarrow a^{2n+1} < 0$, $\forall n \geqslant 0$

Resolução de c):

$n = 0$: $a^{2n+1} = a^1 = a < 0$ (por hipótese).

Seja $r \geqslant 0$ e suponhamos $a^{2r+1} < 0$.

$n = r + 1$: $a^{2(r+1)+1} = a^{(2r+1)+2} = a^{2r+1} \cdot a^2$.

Como $a^{2r+1} < 0$, pela hipótese de indução, e como $a^2 > 0$ (pois $a \neq 0$), então $a^{2r+1} \cdot a^2 < 0$. Donde $a^{2(r+1)+1} < 0$.

157. Sejam a_1 e t elementos de $\mathbb{Z}$ e consideremos $x = a_1t + 1$. Mostre que para todo $n \geqslant 0$ existe $a_n \in \mathbb{Z}$ de modo que $x^n = a_nt + 1$.

158. Sejam a_1 e t elementos de $\mathbb{Z}$ e consideremos $x = a_1t - 1$. Mostre que para todo ímpar $n \geqslant 1$ existe $a_n \in \mathbb{Z}$ para o qual $x^n = a_nt - 1$.

Resolução (por indução sobre n):

$$n = 1: x^1 = (a_1t - 1)^1 = a_1t - 1$$

Seja $r \geqslant 0$ e suponhamos $x^{2r+1} = a_kt - 1$, onde $k = 2r + 1$.

Então: $x^{2(r+1)+1} = x^{2r+3} = x^{2r+1} \cdot x^2 = (a_kt - 1)(a_1t - 1)^2 = (a_kt - 1)$

$(a_1^2t^2 - 2a_1t + 1)$. Podemos fazer $a_1^2t^2 - 2a_1t + 1 = (a_1^2t - 2a_1)t + 1 = a_st + 1$, onde $a_s = a_1^2t - 2a_1$. Logo

$$x^{2(r+1)+1} = x^{2r+3} = (a_kt - 1)(a_st + 1) = a_mt - 1,$$

onde $a_m = a_ka_st + a_k - a_s$.

159. Se $a, b \in \mathbb{Z}$, prove por indução sobre n que $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$, para todo $n \geqslant 1$.

160. Sejam a e b números inteiros ($a \neq 0$ ou $b \neq 0$). Prove que $a^2 + ab + b^2 > 0$.

Sugestão: Para o caso $a > 0$ e $b < 0$ (ou vice-versa), acrescente $0 = ab - ab$ à expressão $a^2 + ab + b^2$ e leve em conta que $ab < 0$ (logo $-(ab) > 0$).

161. Para quaisquer $a, b \in \mathbb{Z}$, prove que: $a < b \Rightarrow a^3 < b^3$.

Sugestão: Usar os exercícios 159 e 160.

162. Se $a, b \in \mathbb{Z}$, prove que: $a^5 = b^5 \Rightarrow a = b$.

163. Se $x \in \mathbb{Z}$, $x \neq 0$, prove que $x^{2n+1} + 1 = (x + 1)(x^{2n} - x^{2n-1} + \ldots - x + 1)$, para todo $n \geqslant 0$.

Resolução (por indução sobre n):

$n = 0$: $x^{2 \cdot 0+1} + 1 = x^1 + 1 = x + 1$; o segundo membro neste caso é $(x + 1) \cdot 1$. Logo, vale a propriedade para $n = 0$.

Seja $r \geqslant 0$ e suponhamos

$$x^{2r+1} + 1 = (x + 1)(x^{2r} - x^{2r-1} + \ldots - x + 1)$$

Multiplicando a igualdade anterior por x^2:

$$x^{2r+3} + x^2 = (x + 1)(x^{2r+2} - x^{2r+1} + \ldots - x^3 + x^2)$$

Somando 1 a ambos os membros e passando x^2 para o segundo:

$$x^{2r+3} + 1 = (x + 1)(x^{2r+2} - x^{2r+1} + \ldots - x^3 + x^2) - (x^2 - 1)$$

Daí:

$$x^{2r+3} + 1 = (x + 1)(x^{2r+2} - x^{2r+1} + \ldots - x^3 + x^2) - (x + 1)(x - 1) =$$
$$= (x + 1)(x^{2r+2} - x^{2r+1} + \ldots - x^3 + x^2 - x + 1)$$

164. Sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Prove que:

a) $\left|\sum_{i=1}^{n} a_i\right| \leqslant \sum_{i=1}^{n} |a_i|$; b) $\left|\prod_{i=1}^{n} a_i\right| = \prod_{i=1}^{n} |a_i|$

165. Um subconjunto S de $\mathbb{Z}$, $S \neq \emptyset$, se diz *limitado superiormente* se $\exists k \in \mathbb{Z}$ de modo que $x \leqslant k$, para todo $x \in S$. Cada elemento k nessas condições chama-se *cota superior* de S. Uma cota superior de S que pertença a S chama-se *máximo* de S. Se m e m' são máximos de S, então $m \leqslant m'$ e $m' \leqslant m$. Daí $m = m'$. Notação: $m = \max S$.
Isso posto, prove que todo subconjunto S de $\mathbb{Z}$, $S \neq \emptyset$, limitado superiormente, possui máximo.

Sugestão: Seja $S' = \{x \in \mathbb{Z} \mid -x \in S\}$. Mostre que S' admite cotas inferiores e que $-(\min S') = \max S$.

166. Seja $a \in \mathbb{Z}$ e indiquemos por $P_{(n)}$ uma propriedade (verdadeira ou falsa) associada a cada $n \leqslant a$. Suponhamos que: i) $P_{(a)}$ é verdadeira; ii) $\forall n \leqslant a$, se $P_{(n)}$ é verdadeira, então $P_{(n-1)}$ também o é. Prove que $P_{(n)}$ é verdadeira para todo $n \leqslant a$.

167. Seja $n \in \mathbb{Z}$, $n \neq 0$. a) Se $n > 0$, mostre que $n = 1 + 1 + \ldots + 1$ (n parcelas). b) Se $n < 0$, mostre que $n = (-1) + (-1) + \ldots + (-1)$, onde o número de parcelas é $p = -n$.

168. Seja $f = \mathbb{Z} \to \mathbb{Z}$ uma função tal que $f(a + b) = f(a) + f(b)$, para quaisquer a, $b \in \mathbb{Z}$. Prove que: a) $f(0) = 0$; b) $f(-a) = -f(a)$, para todo $a \in \mathbb{Z}$; c) $f\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} f(a_i)$, para quaisquer $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ $(n \geqslant 1)$; d) Dê exemplos de funções $f: \mathbb{Z} \to \mathbb{Z}$ para as quais se verifique a condição enunciada.

169. Mostre que para uma função $f: \mathbb{Z} \to \mathbb{Z}$ vale a condição $f(a + b) = f(a) + f(b)$, para quaisquer a, $b \in \mathbb{Z}$, se e somente se $f(n) = f(1)n$, para todo $n \in \mathbb{Z}$.

Sugestão: Decompor $n \neq 0$ segundo o exercício 167 (isso para estabelecer a condição necessária).

170. Mostre que a função $f: \mathbb{Z} \to \mathbb{N}$ definida por $f(n) = 2n$ se $n \geqslant 0$ e $f(n) = (-2)n - 1$ se $n < 0$ é bijetora.

171. a) Mostre que, para todo $n \geqslant 1$:

$$(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \ldots + n)(10 - 1) + (n + 1) = \frac{10^{n+1} - 1}{9}$$

b) Use a) para justificar a seguinte curiosa seqüência de resultados relativa ao nosso sistema de numeração:

$$\begin{aligned} 1 \cdot 9 + 2 &= 11 \\ 12 \cdot 9 + 3 &= 111 \\ 123 \cdot 9 + 4 &= 1111 \\ 1234 \cdot 9 + 5 &= 11111 \\ 12345 \cdot 9 + 6 &= 111111 \\ &\vdots \end{aligned}$$

6. Aritmética em $\mathbb{Z}$

6.1 Múltiplos e divisores

DEFINIÇÃO 2 Diz-se que um número inteiro a *divide* um inteiro b se $b = ac$ para algum $c \in \mathbb{Z}$. Quando isto acontece também se diz que a *é divisor* de b ou que b é *múltiplo* de a (ou *divisível* por a).

Usaremos a notação $a \mid b$ para indicar que a divide b e $a \nmid b$ no caso contrário. O elemento c tal que $b = ac$ é chamado *quociente* de b por a e indicado por $c = \frac{b}{a}$ (eventualmente $b : a$).

Por exemplo: $1 \mid 0$, $-2 \mid +2$, $0 \mid 0$, $3 \nmid -5$.

Em $\mathbb{Z}$ o conjunto dos múltiplos de um dado elemento a será também indicado por M_a e é assim constituído:

$$M_a = \{0, \pm a, \pm 2a, \pm 3a, \ldots\} = M_{(-a)}$$

Por exemplo:

$$M_0 = \{0\}, \ M_1 = M_{(-1)} = \mathbb{Z}$$
$$M_2 = \{0, \pm 2, \pm 4, \pm 6, \ldots\} = M_{-2}$$
$$M_3 = \{0, \pm 3, \pm 6, \pm 9, \ldots\} = M_{-3}$$

Os elementos de M_2 são os *números pares* de $\mathbb{Z}$. É claro que os ímpares de $\mathbb{Z}$ são os elementos de $\mathbb{Z} - M_2 = \{\pm 1, \pm 3, \pm 5, \ldots\}$. Em resumo:

$$M_2 = \{2k \mid k \in \mathbb{Z}\}$$
$$\mathbb{Z} - M_2 = \{2k + 1 \mid k \in \mathbb{Z}\}$$

As propriedades da relação "$x \mid y$" em $\mathbb{Z}$ praticamente são as mesmas da relação análoga em $\mathbb{N}$. Daí porque não nos deteremos em demonstrações, salvo onde houver especificidades.

d_1 $a|a$ (reflexiva)

d_2 $a|b$ e $b|a \Rightarrow a = \pm b$

Por hipótese $b = ac_1$ e $a = bc_2$ e portanto $a = a(c_1c_2)$. É claro que se $a = 0$ então $b = 0$ e portanto o resultado vale neste caso. Se $a \neq 0$, então $c_1c_2 = 1$, do que resulta $c_1 = c_2 = 1$ ou $c_1 = c_2 = -1$ (por quê?). Donde $b = \pm a$.

d_3 $a|b$ e $b|c \Rightarrow a|c$ (transitiva)

d_4 $a|b$ e $a|c \Rightarrow a|(bx + cy)$, $\forall x, y \in \mathbb{Z}$

Em particular: $a|b \Rightarrow a|bx$, $\forall x \in \mathbb{Z}$.

d_5 $a|b \Longleftrightarrow |a|\,|\,|b|$

($\Rightarrow$) Por hipótese $b = ac$, $c \in \mathbb{Z}$. Daí $|b| = |ac| = |a|\,|c|$, o que implica $|a|\,|\,|b|$.

($\Leftarrow$) Por hipótese $|b| = |a|c$, $c \in \mathbb{Z}$. Como $|b| \geqslant 0$ e $|a| \geqslant 0$, então se pode concluir que $c \geqslant 0$ e portanto $c = |c|$. Assim: $|b| = |a|\,|c| = |ac|$. Mas $|b| = \pm b$ e $|ac| = \pm ac = a(\pm c)$. Logo $b = a(\pm c)$ e daí $a|b$.

d_6 Se $a = b + c$ e $d|c$, então: $d|a \Longleftrightarrow d|b$.

6.2 Algoritmo da divisão em $\mathbb{Z}$ (ou algoritmo de Euclides)

Seja b um inteiro estritamente positivo. Se $a \in \mathbb{Z}$, mostremos que existe $n \in \mathbb{N}^*$ de modo que $nb > a$. De fato, tomemos $n = |a| + 1$. Como $b \geqslant 1$, então:

$$nb \geqslant n = |a| + 1 > a$$

Logo é não vazio o conjunto.

$$S = \{n \in \mathbb{N}^* \mid nb > a\}$$

Observando que $S \subset \mathbb{N}^*$, então 0 é uma cota inferior de S. Assim, pelo princípio do menor inteiro existe $q + 1 = \min(S)$. Então:

$$qb \leqslant a < (q + 1)b$$

Somando $-(qb)$ a cada um dos termos:

$$0 \leqslant a - qb < b$$

Pondo $a - qb = r$, então:

$$a = qb + r, \text{ onde } 0 \leqslant r < b$$

Pode-se provar ainda, de maneira análoga ao que foi feito em 4.2 (capítulo II), que q e r, nessas condições, estão univocamente determinados.

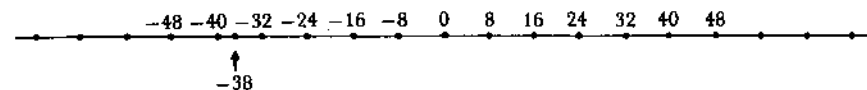
Assim chegamos ao

TEOREMA 1 (algoritmo da divisão em $\mathbb{Z}$ ou algoritmo de Euclides): Para quaisquer $a, b \in \mathbb{Z}$, $b > 0$, existe um único par de inteiros q e r, de maneira que $a = bq + r$, onde $0 \leqslant r < b$.

Na igualdade que expressa o teorema, os elementos a, b, q e r são chamados respectivamente *dividendo, divisor, quociente* e *resto* na divisão euclidiana de a por b.

Exemplo 3: Apliquemos o algoritmo aos números $a = -38$ e $b = 8$. Observemos que o primeiro múltiplo de 8 que supera -38 é -32.

−48 −40 −32 −24 −16 −8 0 8 16 24 32 40 48

↑ −38

Ou seja: $-32 = (q + 1) \cdot 8$, o que implica $q = -5$. Daí:

$$r = a - qb = -38 - (-5) \cdot 8 = 2$$

Assim: $-38 = 8 \cdot (-5) + 2$, onde -5 é o quociente e 2 o resto.

EXERCÍCIOS

172. Ache o quociente e o resto na divisão euclidiana de a por b nos seguintes casos:

a) $a = 390$, $b = 74$ b) $a = -124$, $b = 18$ c) $a = -420$, $b = 58$

173. Na divisão de 326 pelo inteiro $b > 0$, segundo o algoritmo de Euclides, o quociente é 14 e o resto é r. Ache os possíveis valores de b e r.

174. Na divisão euclidiana de -345 por um inteiro $b > 0$, o resto é 12. Ache o divisor e o quociente em todos os casos possíveis.

Resolução: $-345 = b \cdot q + 12$ $(12 < b)$. Daí $-357 = bq$ $(b > 12)$. Donde as possibilidades são as seguintes: $b = 17$ e $q = -21$ ou $b = 21$ e $q = -17$.

175. Na divisão euclidiana de a por b o quociente é 6 e o resto, o menor possível. Ache a e b nos seguintes casos:

a) $a - b = 525$

b) $a + b = 234$.

176. Qual o maior número natural de quatro algarismos divisível por 19? E qual o menor?

177. Prove que:

a) $8^n - 3^n$ é múltiplo de 5, $\forall n \geqslant 0$

b) $64 | (3^{2n+2} - 8n - 9)$, $\forall n \geqslant 0$

c) $7 | (3^{2n+2} - 2^{n+1})$, $\forall n \geqslant 0$

d) $9 | (2^{2n} + 15n - 1)$, $\forall n \geqslant 0$

178. Sejam a, b, c inteiros tais que $a | (b - 3c)$ e $a | (3b - 4c)$. Mostre que $a | c$. Pode-se concluir também que $a | b$? Justifique a resposta.

179. Seja m um inteiro ímpar. Mostre que o resto da divisão de m por 4 é 1 ou 3.

Resolução: Vamos supor $m = 2n + 1$. Se r é o resto na divisão de m por 4, então:

$$2n + 1 = 4q + r \ \ (r = 0, 1, 2 \text{ ou } 3)$$

Para $r = 0$ ou $r = 2$, o segundo membro dessa igualdade seria par, o que não é possível.

180. Sejam m, n inteiros quaisquer. Mostre que:

a) m é par se, e somente se, $m + 2n$ é par.

b) $m + n$ é ímpar se, e somente se, $m - n$ é ímpar.

181. Seja a um inteiro. Mostre que:

a) Um dos inteiros a, $a + 1$, $a + 2$ é divisível por 3.

b) Um dos inteiros a, $a + 2$, $a + 4$ é divisível por 3.

c) Um dos inteiros a, $a + 1$, $a + 2$, $a + 3$ é divisível por 4.

Resolução de b): Devido ao algoritmo de Euclides, $a = 3k$, $a = 3k + 1$ ou $a = 3k + 2$. No primeiro caso $3 | a$; no segundo $a + 2 = 3k + 1 + 2 = 3(k + 1)$ e portanto $3 | (a + 2)$; por fim, se $a = 3k + 2$, então $a + 4 = 3k + 6 = 3(k + 2)$ e $3 | (a + 4)$.

182. Seja m um inteiro cujo resto da divisão por 6 é 5. Mostre que o resto da divisão de m por 3 é 2.

183. Se o resto na divisão euclidiana de m por 8 é 5, qual o resto na divisão de m por 4?

184. Sejam m e n inteiros ímpares. Prove que:

a) $4 | (2m - 2n)$

b) $8 | (m^2 - n^2)$

c) $8 | (m^2 + n^2 - 2)$

185. Mostre que $r | [(r + 1)^n - 1]$, para todo $r \geqslant 2$ e todo $n \geqslant 1$.

186. Prove que, para todo $n \geqslant 0$:

a) $7 | (2^{3n} - 1)$

b) $8 | (3^{2n} + 7)$

c) $3 | [2^n + (-1)^{n+1}]$

187. Mostre que a diferença entre os quadrados de dois inteiros consecutivos é sempre um número ímpar. E a diferença entre os cubos de dois inteiros consecutivos?

188. Seja m um inteiro.

a) Mostre que o resto da divisão de m^2 por 3 é 0 ou 1.

b) Se m é ímpar, mostre que o resto da divisão de m^2 por 4 é 1.

Resolução de b): Como $m = 2k + 1$, então $m^2 = 4k^2 + 4k + 1 = 4 \cdot q + 1$ $(q = k^2 + k)$. Pela unicidade do resto r da divisão em tela, $r = 1$.

189. Se a é um inteiro não divisível por 2 e nem por 3, prove que $24 | (a^2 + 23)$.

190. Demonstre que: para que $a^3 - b^3$ seja múltiplo de 3 é necessário e suficiente que $a - b$ seja múltiplo de 3.

191. Se $10a + b$ é múltiplo de 7, prove que $a^3 - b^3$ também o é.

192. Seja a um inteiro tal que $2 \nmid a$ e $3 \nmid a$. Prove que $24 | (a^2 - 1)$.

Resolução: Aplicando o algoritmo da divisão para a como dividendo e 6 como divisor: $a = 6r + s$ $(s = 0, 1, 2, 3, 4 \text{ ou } 5)$. Como $2 \nmid a$ e $3 \nmid a$, então $s = 1$ ou $s = 5$. No primeiro caso: $a^2 - 1 = (6r + 1)^2 - 1 = 36r^2 + 12r = 12r(3r + 1)$. Se r é par, então 12r é múltiplo de 24 e o mesmo se pode dizer, portanto, de $a^2 - 1$; se r é ímpar, então $3r + 1$ é par, daí $24 | (a^2 - 1)$. O caso $s = 5$ pode ser enfrentado pela mesma linha de raciocínio.

6.3 Máximo divisor comum

DEFINIÇÃO 3 Sejam a e b números inteiros quaisquer. Entendemos por *máximo divisor comum* de a e b e indicamos por mdc(a, b) o número inteiro positivo definido por:

$$\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$$

onde o segundo membro indica, obviamente, o máximo divisor comum de $|a|$ e $|b|$ em $\mathbb{N}$.

Que mdc(a, b) existe e é único, para quaisquer $a, b \in \mathbb{N}$, fato já implícito na definição 3, decorre da teoria do máximo divisor comum em $\mathbb{N}$ (item 6, cap. II). Outra conseqüência é que mdc(a, b) = mdc(a, b), para todo par de elementos $a, b \in \mathbb{Z}$.

Se mdc(a, b) = 1, diz-se que a e b são *primos entre si* ou que a é *primo com* b (ou vice-versa).

Por exemplo:

$$\text{mdc}(-4, 6) = \text{mdc}(4, 6) = 2$$
$$\text{mdc}(-2, -3) = \text{mdc}(2, 3) = 1$$
$$\text{mdc}(0, -4) = \text{mdc}(0, 4) = 4$$

PROPOSIÇÃO 4 Um número d é o máximo divisor comum de a e b ($a, b \in \mathbb{Z}$) se, e somente se:

i $d \geqslant 0$

ii $d|a$ e $d|b$

iii $c|a$ e $c|b \Rightarrow c|d$

Demonstração:

($\Rightarrow$) Como $d = \text{mdc}(a, b) = \text{mdc}(|a|, |b|)$, então $d \geqslant 0$. Por hipótese $d \mid |a|$ e $d \mid |b|$, o que implica $d|a$ e $d|b$. Finalmente, se $c|a$ e $c|b$, então $|c| \mid |a|$ e $|c| \mid |b|$, do que segue $|c| \mid \text{mdc}(|a|, |b|)$. Daí, $c|d$.

($\Leftarrow$) Como $d|a$ e $d|b$, então $d \mid |a|$ e $d \mid |b|$. Se $c \mid |a|$ e $c \mid |b|$, então $c|a$ e $c|b$; daí $c|d$, devido a iii. ■

PROPOSIÇÃO 5 Se $a|b$, então $\text{mdc}(a, b) = |a|$.

Demonstração: i Obviamente $|a| \geqslant 0$. ii Como $a = |a|(\pm 1)$, então a é múltiplo de $|a|$; e como $a|b$, então $|a| \mid b$. iii Se $c|a$ e $c|b$, então $c \mid |a|$.

PROPOSIÇÃO 6 Se $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

A ***demonstração*** desta última proposição é análoga à da proposição 2 (item 6, cap. II) — por isso não a faremos.

As proposições 5 e 6 servem de base para a determinação de mdc(a, b) pelo processo das divisões sucessivas, também no caso presente. Por exemplo, se $a = -26$ e $b = 18$:

	1	2	4
26	18	8	(2)
8	2	0	

A explicação (justificativa) do processo também consta do item 6, capítulo II. Assim:

$$\text{mdc}(-26, 18) = \text{mdc}(26, 18) = 2$$

PROPOSIÇÃO 7 Se $d = \text{mdc}(a, b)$, então existem $x_0, y_0 \in \mathbb{Z}$ de maneira que

$$d = ax_0 + by_0$$

Demonstração: Se $a = b = 0$, então $d = 0$ e qualquer par x_0, y_0 satisfaz $0 = 0x_0 + 0y_0$.

Se $a \neq 0$ ou $b \neq 0$ (ou ambos), seja:

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}$$

Como $a \cdot a + b \cdot b = a^2 + b^2 \in S$ e $a^2 + b^2 > 0$ (pois $a \neq 0$ ou $b \neq 0$), então em S há elementos estritamente positivos. Se d é o menor desses inteiros, mostremos que $d = \text{mdc}(a, b)$. De fato:

ii Como $d \in S$, então existem $x_0, y_0 \in \mathbb{Z}$ de modo que $d = ax_0 + by_0$. Aplicando o algoritmo da divisão aos elementos a e d

$$a = dq + r \quad (0 \leqslant r < d)$$

Substituindo d nesta igualdade pelo segundo membro da igualdade anterior:

$$a = (ax_0 + by_0)q + r$$

e então:

$$r = a(1 - qx_0) + b[q(-y_0)]$$

de onde se conclui que $r \in S$. Sendo r positivo e levando em conta que d é o menor dos elementos estritamente positivos de S, então $r = 0$. Donde $a = dq$ e $d|a$. Analogamente se prova que $d|b$.

iii Como $d = ax_0 + by_0$, todo divisor c de a e b é divisor de d. ■

COROLÁRIO 1 Dois números a e b são primos entre si se, e somente se, existem x_0, $y_0 \in \mathbb{Z}$ de maneira que $ax_0 + by_0 = 1$.

Demonstração:

($\Rightarrow$) É a proposição 7 para $d = 1$.

($\Leftarrow$) É claro que $1 > 0$ e que $1|a$ e $1|b$. Agora, se $c|a$ e $c|b$, então $c|(ax_0 + by_0)$, ou seja, $c|1$. ■

Exemplo 4: Os elementos x_0, y_0 cuja existência a proposição anterior garante não estão univocamente determinados. Mas o processo das divisões sucessivas nos permite encontrar sempre uma solução para esse problema quando $a \neq 0$ e $b \neq 0$ (os demais casos são imediatos). Sejam por exemplo $a = -26$ e $b = 18$. Como já vimos:

$$\begin{aligned} 26 &= 18 \cdot 1 + 8 \\ 18 &= 8 \cdot 2 + 2 \\ 8 &= 2 \cdot 4 \end{aligned}$$

onde destacamos os elementos principais do processo. Como $mdc(26, 18) = 2$, toma-se a igualdade onde o resto é 2 e faz-se:

$$2 = 18 - 8 \cdot 2$$

Como $8 = 26 - 18 \cdot 1$ (o que sai da primeira das igualdades anteriores), então:

$$2 = 18 - (26 - 18 \cdot 1) \cdot 2 = 26(-2) + 18 \cdot 3$$

Isto mostra que $(-2, 3)$ é solução de

$$26x + 18y = 2$$

Portanto, $x_0 = 2$ e $y_0 = 3$ são uma solução de $(-26)x + 18y = 2$.

Observe-se que, por exemplo, $(20, 29)$ também é solução de $(-26)x + 18y = 1$. Ainda neste capítulo (7) mostraremos como achar o conjunto das soluções de $ax + by = c$ $(a, b, c \in \mathbb{Z})$.

COROLÁRIO 2 Se a e b estão em $\mathbb{Z}$, $a \neq 0$ ou $b \neq 0$, e se $d = mdc(a, b)$, então:

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Neste caso é possível uma *demonstração* mais elegante que em $\mathbb{N}$. Da hipótese decorre que existem x_0, $y_0 \in \mathbb{Z}$ para os quais $ax_0 + by_0 = d$. Daí:

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1$$

o que, pelo corolário anterior, garante a tese. ■

COROLÁRIO 3 Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.

Por hipótese existem x_0, $y_0 \in \mathbb{Z}$ de modo que $ax_0 + by_0 = 1$. Daí $(ac)x_0 + (bc)y_0 = c$. Como a divide o primeiro membro (pois é fator de ac e divide bc, por hipótese), então $a|c$. ■

COROLÁRIO 4 Se a e b são divisores de $c \neq 0$ e $mdc(a, b) = 1$, então $ab|c$.

Deixamos a demonstração como exercício. A idéia é, mais uma vez, usar o corolário 1.

Nota: O conceito de máximo divisor comum pode ser estendido para três ou mais números inteiros, por recorrência, assim:

$$mdc(a_1, a_2, \ldots, a_n) = mdc(mdc(a_1, a_2, \ldots, a_{n-1}), a_n)$$

Nessas condições $d \in \mathbb{Z}$ é o máximo divisor comum de $a_1, \ldots, a_n$ se, e somente se, **i** $d \geq 0$; **ii** $d|a_i (i = 1, 2, \ldots, n)$; **iii** $c|a_i (i = 1, 2, \ldots, n) \Rightarrow c|d$.

Por exemplo: $mdc(-6, -4, 8) = mdc(mdc(-6, -4), 8) =$
$= mdc(mdc(6, 4), 8) = mdc(2, 8) = 2.$

6.4 Mínimo múltiplo comum

DEFINIÇÃO 4 Dados $a, b \in \mathbb{Z}$, existe e é único o mínimo múltiplo comum m de $|a|$ e $|b|$ em $\mathbb{N}$. O número m é chamado também *mínimo múltiplo comum* de a e b. Notação: $m = mmc(a, b)$.

Da teoria do mínimo múltiplo comum em $\mathbb{N}$ decorre que $mmc(a, b) = mmc(b, a)$.

Seja $m = mmc(a, b)$. Notemos o seguinte:

i $m \geq 0$ pois m é o mmc de $|a|$ e $|b|$ em $\mathbb{N}$.

ii Como m é múltiplo de $|a|$ e de $|b|$, então m é múltiplo de a e b.

iii Se m' é múltiplo de a e b, também o é de $|a|$ e de $|b|$ e portanto é múltiplo de m, pois $m = mmc(|a|, |b|)$ (em $\mathbb{N}$).

Reciprocamente, seja $m \geq 0$ um inteiro múltiplo de a e de b, tal que todo múltiplo comum de a e b também o é de m. Isto posto: a) m é múltiplo de

$|a|$ e de $|b|$; b) se m' é múltiplo de $|a|$ e $|b|$, m' é múltiplo de a e b e portanto é múltiplo de m. Logo m é o mmc de $|a|$ e $|b|$ em $\mathbb{N}$ e então o mmc de a e b em $\mathbb{Z}$.

PROPOSIÇÃO 8 Para quaisquer $a, b \in \mathbb{Z}$:

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = |a|\,|b| = |ab|$$

Em particular, se $a \neq 0$ ou $b \neq 0$, então:

$$\text{mmc}(a, b) = \frac{|ab|}{\text{mdc}(a, b)}$$

Demonstração: De fato, levando em conta a proposição 4, capítulo II:

$$\text{mdc}(|a|, |b|)\ \text{mmc}(|a|, |b|) = |a|\,|b| = |ab|$$

Agora é só levar em conta que

$$\text{mdc}(|a|, |b|) = \text{mdc}(a, b) \text{ e } \text{mmc}(|a|, |b|) = \text{mmc}(a, b)$$

E se $a \neq 0$ ou $b \neq 0$, então $\text{mdc}(a, b) = \text{mdc}(|a|, |b|) \neq 0$. Logo:

$$\text{mdc}(a, b)\ \text{mmc}(a, b) = |ab| \Rightarrow \text{mmc}(a, b) = \frac{|ab|}{\text{mdc}(a, b)} \qquad \blacksquare$$

Por exemplo, como $\text{mdc}(-26, 8) = 2$ (exemplo 4), então

$$\text{mmc}(-26, 8) = \frac{|-26|\,|8|}{2} = 4 \cdot 26 = 104$$

Nota: Se $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ $(n > 2)$, então pode-se definir o mínimo múltiplo comum desses elementos, por recorrência, do seguinte modo:

$$\text{mmc}(a_1, a_2, \ldots, a_n) = \text{mmc}(a_1, \text{mmc}(a_2, a_3, \ldots, a_n))$$

Isso posto, um elemento $m \in \mathbb{Z}$ é mínimo múltiplo comum de $a_1, a_2, \ldots, a_n$ se, e somente se:

i $m \geqslant 0$; **ii** $a_i | m$ $(i = 1, 2, \ldots, n)$; **iii** $a_i | m'$ $(i = 1, 2, \ldots, n) \Rightarrow m | m'$.

Por exemplo: $\text{mmc}(-6, 10, -12) = \text{mmc}(-6, \text{mmc}(10, -12)) = \text{mmc}(6, \text{mmc}(10, 12)) = \text{mmc}(6, 60) = 60$.

EXERCÍCIOS

193. Calcule:

a) $\text{mmc}(-120, 68)$
b) $\text{mdc}(0, -204)$
c) $\text{mdc}(-68, -250)$
d) $\text{mmc}(20, -74)$
e) $\text{mmc}(-42, -54)$
f) $\text{mmc}(-20, 77, -120)$

194. Se $a = -5^2 \cdot 41$, $b = 3^2 \cdot 5 \cdot 19$ e $c = -13$, determine:

a) $\text{mdc}(a, b)$
b) $\text{mmc}(b, c)$
c) $\text{mdc}(a, b, c)$
d) $\text{mmc}(a, b, c)$

195. Se $A = \{x \in \mathbb{Z} \mid \text{mdc}(x, 2) = 1\}$ e $B = \{x \in \mathbb{Z} \mid \text{mdc}(x, 3) = 1\}$, ache $A \cap B$.

196. Se n é inteiro, quais os possíveis valores de $\text{mdc}(n, n + 7)$?

197. Encontre os valores possíveis de b em $\mathbb{Z}$ de maneira que:

a) $\text{mdc}(63 - b, b) = 9$
b) $\text{mdc}(20 + b, b) = 4$
c) $\text{mmc}(b, b + 15) = 180$
d) $\text{mdc}\left(\frac{576}{b}, b\right) = 8$

198. a) Se n é um inteiro par, prove que $\text{mdc}(n, n + 2) = 2$.
b) Se n é ímpar, prove que $\text{mdc}(n, n + 2) = 1$.

Resolução de b): Seja $d = \text{mdc}(n, n + 2)$. Então $d | n$, $d | (n + 2)$ e portanto $d | 2$. Logo $d = 1$ ou $d = 2$. Mas como n é ímpar, então d não pode ser igual a 2. Donde $d = 1$.

199. Sejam a e b inteiros primos entre si. Prove que $\text{mmc}(a, b) = |ab|$.

200. Sejam $a, b \in \mathbb{Z}$. Prove que: $\text{mdc}(a, b) = 1 \Longleftrightarrow \text{mdc}(a + b, b) = 1$.

201. Sejam a, b e c três inteiros assim relacionados: $c = ab + 1$. Prove que $\text{mdc}(a, c) = \text{mdc}(b, c) = 1$.

202. Sejam a, b e c inteiros arbitrários. Se $\text{mdc}(a, b) = 1$ e $c | (a + b)$, prove que $\text{mdc}(a, c) = \text{mdc}(b, c) = 1$.

Resolução: Seja $d = \text{mdc}(a, c)$. Então $d | a$, $d | c$ e, como $c | (a + b)$, então $d | (a + b)$. Logo $d | b$, pois $b = (a + b) - a$. Conseqüentemente $d | 1$, pois $1 = \text{mdc}(b, c)$.

203. Sejam a e b inteiros primos entre si. Prove que $\text{mdc}(a + b, a - b) = 1$ ou $\text{mdc}(a + b, a - b) = 2$.

204. Mostre que $\text{mdc}(a, b) = \text{mdc}(a, b, a + b)$, para quaisquer $a, b \in \mathbb{Z}$.

205. Seja c um inteiro ímpar. Se c é um divisor de $a + b$ e de $a - b$, mostre que c também é um divisor de $d = \text{mdc}(a, b)$.

206. Considere os inteiros a, b e c. Se $a | c$, $c | b$ e $\text{mdc}(a, b) = 1$, prove que $a = \pm 1$.

207. Para dois inteiros quaisquer a e b, prove que $mdc(a, b) = mdc(5a + 3b, 13a + 8b)$.

208. Se $mdc(m, b, c) = 1$, prove que $mdc(a, b, c) = mdc(ma, b, c)$, para qualquer $a \in \mathbf{Z}$.

Resolução: Seja $d = mdc(a, b, c)$. Obviamente $d \geqslant 0$ e $d|(ma)$, $d|b$ e $d|c$. Seja r um divisor comum a ma, b e c e mostremos que $mdc(r, m) = 1$. De fato, se $s|r$ e $s|m$, então $s|b$, $s|c$ e $s|m$ e daí $s = \pm 1$, devido à hipótese. Como $r|(ma)$, o fato de $mdc(r, m) = 1$ implica $r|a$. Logo, $r|a$, $r|b$ e $r|c$ e portanto $r|d$.

209. Para todo inteiro n, prove que $n(n + 1)$ e $n + 2$ são primos entre si se n é ímpar e $mdc(n(n + 1), n + 2) = 2$ se n é par.

210. Se $d = mdc(-68, 42)$, ache dois inteiros x_0 e y_0 de maneira que

$$(-68)x_0 + 42y_0 = d$$

211. Encontre um par de inteiros x_0, y_0 para o qual $(-102)x_0 + (-49)y_0 = 1$.

212. Se a e b são inteiros não nulos, prove que:

a) Existem inteiros x e y para os quais $ax + by = c$ se, e somente se, c é múltiplo de $d = mdc(a, b)$.

b) Se existem $x, y \in \mathbf{Z}$ de maneira que $ax + by = d$, onde $d = mdc(a, b)$, então $mdc(x, y) = 1$.

213. Demonstre que se $a|bc$ e $mdc(a, b) = d$, então $a|cd$.

Resolução: Devido à proposição 7, existem $x_0, y_0 \in \mathbf{Z}$ para os quais $d = ax_0 + by_0$. Daí: $cd = (ac)x_0 + (bc)y_0$. Como $a|(ac)$ e, por hipótese, $a|(bc)$, então $a|cd$.

214. Prove que, se $a|c$, $b|c$ e $mdc(a, b) = d$, então $ab|cd$.

Sugestão: Use a mesma idéia do exercício anterior.

215. Prove que $mdc(a + b, a - b) \geqslant mdc(a, b)$, para quaisquer $a, b \in \mathbf{Z}$.

216. Sejam a e b inteiros primos entre si. Prove que:

a) $mdc(2a + b, a + 2b) = 1$ ou 3

b) $mdc(a + b, a^2 + b^2) = 1$ ou 2

c) $mdc(a + b, a^2 - ab + b^2) = 1$ ou 3

Resolução de a): Seja $d = mdc(2a + b, a + 2b)$. Então $d|(2a + b)$, $d|(2a + 4b)$ e portanto $d|(3b)$. Mas $mdc(d, b) = 1$. De fato, se $r|d$ e $r|b$, então $r|(a + 2b)$ e $r|(2b)$ e daí $r|a$; absurdo pois $mdc(a, b) = 1$. Logo $d|3$, razão pela qual $d = 1$ ou $d = 3$.

217. Se se efetua a divisão euclidiana de 4 373 e de 826 pelo mesmo número $b > 0$, obtêm-se restos 8 e 7, respectivamente. Qual o valor de b?

218. Determine todos os números de três algarismos que são múltiplos, simultaneamente, de 9 e 11.

219. a) Se n é um inteiro arbitrário, prove que $n(2n + 7)(7n + 1)$ é múltiplo de 6.

b) Prove que $ab(a^2 + b^2)(a^2 - b^2)$ é múltiplo de 30, para quaisquer $a, b \in \mathbf{Z}$.

Sugestão para b): Mostrar que a expressão dada é divisível por 5 e por 6.

220. Prove que: $mdc(a, mn) \neq 1 \iff mdc(a, m) \neq 1$ ou $mdc(a, n) \neq 1$.

Resolução:

($\Rightarrow$) Vamos supor $mdc(a, mn) = d > 1$, $mdc(a, m) = 1$ e $mdc(a, n) = 1$. Desta última relação decorre que, para convenientes $x_0, y_0 \in \mathbf{Z}$, $ax_0 + ny_0 = 1$. Daí $amx_0 + mny_0 = m$. Como d divide as parcelas do primeiro membro desta igualdade, $d|m$. Mas $d|a$ e, sendo $1 = mdc(a, m)$, $d = 1$. Absurdo.

($\Leftarrow$) Admitamos, com a hipótese feita, que $mdc(a, mn) = 1$. Logo, para algum par $x_0, y_0 \in \mathbf{Z}$, $ax_0 + mny_0 = 1$. Mas daí segue, simultaneamente, que $mdc(a, m) = mdc(a, n) = 1$ (corolário 1, proposição 7). Absurdo.

221. Prove que o produto de cinco inteiros consecutivos é múltiplo de 120.

222. Se a, m e n são inteiros positivos e n é ímpar, prove que:

$$mdc(a^n - 1, a^m + 1) \leqslant 2$$

Resolução: Seja $d = mdc(a^n - 1, a^m + 1)$. Então $a^n = 1 + kd$ e $a^m = sd - 1$. Daí $(a^n)^m = a^{mn} = 1 + ud$ e $(a^m)^n = a^{mn} = vd - 1$ (ver exercícios 157 e 158). Daí $1 + ud = vd - 1$ e portanto $d(v - u) = 2$. Donde $d|2$, o que implica $d = 1$ ou $d = 2$.

6.5 Números primos

DEFINIÇÃO 5 Um número $p \in \mathbb{Z}$ é chamado *inteiro primo* (ou simplesmente *primo*) se $|p|$ é primo em $\mathbb{N}$.

Por exemplo: -2, -3 e -5 são inteiros primos pois 2, 3 e 5 são primos em $\mathbb{N}$.

PROPOSIÇÃO 9 Seja $p \in \mathbb{Z}$. Então p é um inteiro primo se, e somente se, $p \neq 0$, $p \neq \pm 1$ e os únicos divisores de p são ± 1 e $\pm p$.

Demonstração:

($\Rightarrow$) Se p é primo em $\mathbb{Z}$ então $|p|$ é primo em $\mathbb{N}$. Logo $|p| \neq 0$ e $|p| \neq 1$, o que implica $p \neq 0$ e $p \neq \pm 1$.
Se $a|p$, então $|a|\,\big|\,|p|$ e, devido à hipótese, $|a| = 1$ ou $|a| = p$. Logo $a = \pm 1$ ou $a = \pm p$.

($\Leftarrow$) Se $p \neq 0$ e $p \neq \pm 1$, então $|p| \neq 0$ e $|p| \neq 1$. Se $c \in \mathbb{N}$ e $c\,\big|\,|p|$, então $|p| = cq$ ($q \in \mathbb{N}$) e então $|p| = |cq|$. Daí $p = \pm cq = c(\pm q)$ e portanto $c|p$ (em $\mathbb{Z}$). Pela hipótese $c = \pm 1$ ou $c = \pm p$. Como $c \in \mathbb{N}$, então $c = 1$ ou $c = |p|$. Assim, provamos que $|p|$ é primo em $\mathbb{N}$. Logo p é primo em $\mathbb{Z}$. ∎

PROPOSIÇÃO 10 Sejam a, b e p números inteiros. Se $p|ab$ e p é primo, então $p|a$ ou $p|b$.

A *demonstração* não difere daquela feita para a proposição 6, capítulo II.

TEOREMA 2 (*teorema fundamental da aritmética em $\mathbb{Z}$*): Seja $a \in \mathbb{Z}$, $a \neq 0$ e $a \neq \pm 1$. Então existem números primos $p_1, p_2, \ldots, p_r \in \mathbb{Z}$ ($r \geqslant 1$), todos maiores que 1, de maneira que:

$$a = p_1 p_2 \ldots p_r \qquad \text{ou} \qquad a = -p_1 p_2 \ldots p_r$$

conforme $a > 0$ ou $a < 0$. Ademais essa decomposição, a menos da ordem dos fatores, é única.

A *demonstração* é imediata. No que tange à existência, basta considerar que $a = \pm|a|$ e aplicar o teorema fundamental da aritmética (teorema 3, cap. II) ao número natural $|a|$. Quanto à unicidade, o raciocínio é o mesmo empregado no referido teorema. ∎

Por exemplo:

$$-100 = -2^2 \cdot 5^2$$
$$-105 = -3 \cdot 5 \cdot 7$$

Um número inteiro $a \neq 0$, $a \neq \pm 1$ que não é primo chama-se *composto*.

Obviamente a é composto se, e somente se, $-a$ é composto. Se a é composto, então existem $b, c \in \mathbb{Z}$, $1 < b, c < |a|$, de modo que $a = \pm(bc)$. De fato, como $a \neq 0$ e $a \neq \pm 1$, então a admite um divisor primo $b > 1$. Daí $a = bq$, onde $q \in \mathbb{Z}$ e $q \neq \pm 1$ (pois a não é primo), além de, obviamente, $q \neq 0$. Daí $|q| > 1$. Considerando ainda que $|a| = |b|\,|q|$ e $|b| > 1$, então $|q| < |a|$. Assim, basta fazer $c = |q|$.

EXERCÍCIOS

223. Decomponha em fatores primos, segundo o teorema fundamental da aritmética em $\mathbb{Z}$, os seguintes inteiros:

a) $-28\,820$
b) $-1\,324\,413$
c) $-12\,317$
d) $-1\,996$

224. Verifique se são primos os seguintes inteiros:

a) -449
b) -427
c) -511
d) -227

225. Seja p um número primo, $p \neq \pm 2$ e $p \neq \pm 3$. Prove que existe $k \in \mathbb{Z}$ de modo que $p^2 = 24k + 1$.

Sugestão: A hipótese obriga que $p = 6a \pm 1$.

226. Para todo inteiro n, prove que:

$$\text{mdc}(n - 1, n^2 + n + 1) = 1 \text{ ou } 3$$

Resolução: Vamos supor $\text{mdc}(n - 1, n^2 + n + 1) = d > 1$ e seja p um divisor primo de d. Então $p|(n - 1)^2$ e $p|(n^2 + n + 1)$; daí $p|3n$, pois $(n^2 + n + 1) - (n - 1)^2 = 3n$. Como p é primo, então $p|3$ ou $p|n$. Se $p|n$, como $p|(n^2 + n + 1)$, então $p|1$, o que não é possível. Logo $p = 3$ (ou $p = -3$) e o único fator primo positivo de d é 3. Provemos que o expoente de 3 em d é 1, ou seja, que $d = 3$. Se $d = 3^k$ ($k > 1$), então $9|(n - 1)$ e $9|(n^2 + n + 1)$; daí $n = 9r + 1$ e $n^2 + n + 1 = 9s$; logo, $(9r + 1)^2 + (9r + 1) + 1 = 81r^2 + 27r + 3 = 9(9r^2 + 3r) + 3 = 9s$, do que resulta $3(9r^2 + 3r) + 1 = 3s$. Absurdo. Donde, se $d > 1$, então $d = 3$.

227. Determine todos os inteiros primos que podem ser escritos como $n^2 - 1$, para algum $n \in \mathbb{Z}$.

228. Se n é um inteiro e $n^3 - 1$ é primo, mostre que $n = 2$ ou $n = -1$.

229. Para todo inteiro $n > 3$, prove que $n^4 + 4$ é um número composto.

Sugestão: Acrescente $4n^2 - 4n^2$ à expressão e procure fatorar o resultado.

230. Se $n^2 + 2$ é primo, prove que n é múltiplo de 3.

Sugestão: Mostre que são impossíveis as alternativas $n = 3q + 1$ ou $n = 3q + 2$.

231. Se $p \geqslant 5$ é um número primo, prove que $p^2 + 2$ é um número composto.

232. Se o resto da divisão euclidiana de um número primo por 3 é 1, mostre que na divisão desse número por 6 o resto também é 1.

233. Sejam $d_1 = \text{mdc}(a, b_1)$ e $d_2 = \text{mdc}(a, b_2)$. Prove que $\text{mdc}(a, b_1b_2) = \text{mdc}(a, d_1d_2)$.

Sugestão: Se r é um divisor qualquer de b_1b_2, então $r = r_1r_2$, onde r_1 é divisor de b_1 e r_2 é divisor de b_2 — o que é conseqüência do teorema fundamental da aritmética.

234. Seja $n \geqslant 4$ um número inteiro composto. Prove que n divide $(n - 1)!$

Resolução: Sendo n composto, então existem $a, b \in \mathbb{Z}$ de maneira que $1 < a, b \leqslant n - 1$ e $n = ab$. Assim, a e b são fatores de $(n - 1)!$ Se $a \neq b$, é imediato, então, que n divide $(n - 1)!$ Se $a = b$, então $n = a^2 \geqslant 4$, o que implica $a \geqslant 2$. Daí $2a \leqslant a^2 = n$ e portanto 2a também é fator de $(n - 1)!$ Donde

$$(n - 1)! = (n - 1) \ldots (2a) \ldots a \ldots 2 \cdot 1$$

o que mostra que $a^2 | (n - 1)!$

235. Ache dois inteiros a e b, se o primeiro tem 21 divisores, o segundo 10 e $\text{mdc}(a, b) = 1\,250$.

236. Mostre que há uma infinidade de primos da forma $4r + 1$.

Sugestão: Suponha que os primos dessa forma fossem $n: p_1, p_2, \ldots, p_n$. Considere $a = p_1p_2 \ldots p_n + 1$. Os fatores primos de a têm que ser da forma $4n + 3$. Mas isso levará a um absurdo.

237. Ache o menor inteiro positivo n para o qual a função $f(n) = n^2 + n + 17$ fornece um número composto. Faça o mesmo com as funções $g(n) = n^2 + 21n + 1$ e $h(n) = 3n^2 + 3n + 23$.

238. Em 1742 o russo Christian Goldbach formulou a seguinte conjectura (conhecida como *conjectura de Goldbach*): "Todo inteiro par maior que 2 é soma de dois números primos positivos". Por exemplo: $4 = 2 + 2$; $6 = 3 + 3$; $8 = 3 + 5$; $10 = 3 + 7$; $12 = 5 + 7$, etc. Essa ainda é uma questão em aberto na Matemática.
Admitindo a conjectura de Goldbach, prove que todo inteiro par maior que 5 é igual à soma de três números primos positivos.

Sugestão: Se $2n - 2 = p + q$ (p e q primos), então $2n = 2 + p + q$ e $2n + 1 = p + q + 3$.

239. Seja p um número ímpar. Se p e $p + 2$ são números primos, diz-se que p e $p + 2$ são *primos gêmeos*.

a) Mostre que 1 949 e 1 951 são primos gêmeos.

b) Se p e $p + 2$ são primos gêmeos e $p > 3$, mostre que sua soma é múltiplo de 12.

240. Seja $p \neq 5$ um número primo ímpar. Prove que $10 | (p^2 - 1)$ ou $10 | (p^2 + 1)$.

241. Sejam a e b inteiros tais que $\text{mdc}(a, b) = p$, onde p é primo. Prove que $\text{mdc}(a^2, b) = p$ ou p^2.

Resolução: Seja $\text{mdc}(a^2, b) = d$ e indiquemos por q um divisor primo de d. (Note-se que como $p | a^2$ e $p | b$, então $d > 1$.) Como $q | a^2$ e $q | b$, então $q | a$ e $q | b$; daí $q | p$ e portanto $q = p$. Assim $d = p^r$ $(r \geqslant 1)$. Vamos supor que $r > 2$. Então, de um lado, $p^2 | b$. De outro, $p^r | a^2$, o que leva a $a^2 = p^r q$ $(q \in \mathbb{Z})$; mas $p | a$ e então $a = ps$ $(s \in \mathbb{Z})$; assim $p^2s^2 = p^r q$, de onde segue (cancelando p^2) que $p | s$ e portanto (já que $a = ps$) $p^2 | a$. Como porém $\text{mdc}(a, b) = p$, as conclusões a que chegamos ($p^2 | a$ e $p^2 | b$) constituem um absurdo. Logo $r \leqslant 2$.

242. Se $\text{mdc}(a, b) = p$, onde p é primo, mostre que $\text{mdc}(a^3, b) = p$, p^2 ou p^3.

243. Quais os valores possíveis de $\text{mdc}(a^2, b^3)$, se $\text{mdc}(a, b)$ é um número primo? Justifique.

244. a) Ache o expoente de 5 na decomposição de 100! em fatores primos.

b) Qual o expoente de 7 na decomposição de 1 000 em fatores primos? Justifique a resposta.

Resolução de a): Os fatores de $100! = 100 \cdot 99 \cdot \ldots 2 \cdot 1$ em que o 5 figura são 5, 10, 15, ..., 95, 100 (vinte fatores). Observemos que: $5 \cdot 10 \cdot 15 \ldots 95 \cdot 100 = 5^{20} \cdot (1 \cdot 2 \cdot 3 \ldots 19 \cdot 20)$. No produto en-

tre parênteses o 5 figura nos fatores 5, 10, 15 e 20. Como $5 \cdot 10 \cdot 15 \cdot 20 = 5^4 \cdot (1 \cdot 2 \cdot 3 \cdot 4)$, então o expoente de 5 no fatorial 100! é $20 + 4 = 24$.

245. Decomponha em fatores primos, segundo o teorema fundamental da aritmética, o número 50!

Sugestão: Estenda o raciocínio do exercício anterior a todos os fatores primos de 50!

246. Se $\text{mdc}(a, b) = d$, prove que $\text{mdc}(a^2, b^2) = d^2$.

247. Se p e $p^2 + 8$ são ambos números primos, prove que $p^3 + 4$ também é primo.

248. Sejam a e b inteiros primos entre si e n um inteiro tal que $n + 2 = p$ é um número primo. Mostre que:

$$\text{mdc}(a + b, a^2 - nab + b^2) = 1 \text{ ou } |p|$$

249. Se $a = 2^n + 1$ é primo $(n \geqslant 1)$, prove que $n = 2^r$ $(r \geqslant 0)$.

Resolução: Vamos supor que um dos fatores primos de n fosse ímpar. Se $2s + 1$ $(s \neq 0)$ é esse fator, então $n = t(2s + 1)$, onde $t \geqslant 1$, e

$$a = (2^t)^{2s+1} + 1$$

Fazendo $2^t = x$, então $a = x^{2s+1} + 1$. Mas, conforme exercício 163:

$$x^{2s+1} + 1 = (x + 1)(x^{2s} - x^{2s-1} + \ldots - x + 1) = a$$

Absurdo, pois $x + 1 \geqslant 2$ e $x^{2s} - x^{2s-1} + \ldots - x + 1 \geqslant 2$ (por quê?) e a é primo. Se n não possui fatores primos ímpares, então n é potência de 2 (expoente $\geqslant 0$).

7. Equações diofantinas lineares

Diofanto de Alexandria viveu provavelmente no século III d.C. Dele se conhecem duas obras: *Sobre números poligonais* e *Aritmética*. Esta última, da qual restam seis livros (segundo o prefácio o número total de livros seria treze), é a mais importante e original. Trata-se de uma coletânea de problemas, na maioria indeterminados, para cuja resolução Diofanto usa sempre métodos algébricos, com o que se distingue substancialmente da matemática grega clássica.

Devido a essa sua utilização de métodos algébricos, hoje recebem o nome de *equações diofantinas* todas as equações polinomiais (com qualquer número de incógnitas), com coeficientes inteiros, sempre que se trata de procurar suas possíveis soluções também entre os inteiros. Isso embora Diofanto só tenha estudado algumas dessas equações, em casos particulares, e embora o universo que tenha usado para resolução de seus problemas fosse o conjunto dos números racionais positivos.

Neste item estudaremos as *equações diofantinas lineares*, especialmente com duas incógnitas. Consideremos pois uma equação:

$$ax + by = c \quad (1)$$

onde $a, b \in \mathbb{Z}$ e suponhamos a e b não simultaneamente nulos. Uma solução de (1) é, neste contexto, um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ para o qual a igualdade:

$$ax_0 + by_0 = c$$

é verdadeira. Vejamos em que condições (1) admite soluções.

PROPOSIÇÃO 11 Uma equação diofantina $ax + by = c$, em que $a \neq 0$ ou $b \neq 0$, admite solução se, e somente se, $d = \text{mdc}(a, b)$ divide c.

Demonstração:

$(\Rightarrow)$ Se $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ é solução, vale a igualdade:

$$ax_0 + by_0 = c$$

Como $d|a$ e $d|b$, então $d|c$ (propr. $\mathbf{d_4}$).

$(\Leftarrow)$ Como $d = \text{mdc}(a, b)$, a proposição 7 garante que $d = ax_0 + by_0$, para um conveniente par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. Mas da hipótese $d|c$ segue que $c = dt$, para algum $t \in \mathbb{Z}$. Assim

$$c = dt = (ax_0 + by_0)t = a(x_0t) + b(y_0t)$$

o que mostra que (x_0t, y_0t) é solução da equação considerada. ■

PROPOSIÇÃO 12 Seja (x_0, y_0) uma particular solução da equação diofantina $ax + by = c$, onde $a \neq 0$ e $b \neq 0$. Então essa equação admite infinitas soluções e o conjunto dessas soluções é:

$$S = \left\{\left(x_0 + \frac{b}{d}t,\ y_0 - \frac{a}{d}t\right) \middle| t \in \mathbb{Z}\right\}$$

onde $d = \text{mdc}(a, b)$.

Demonstração: Se indicamos genericamente por (x', y') as soluções de $ax + by = c$, então

$$ax' + by' = c = ax_0 + by_0$$

o que equivale a

$$a(x' - x_0) = b(y_0 - y')$$

Daí, supondo $a = dr$ e $b = ds$, vem

$$r(x' - x_0) = s(y_0 - y')$$

onde $\text{mdc}(r, s) = 1$. Como, pela igualdade anterior, r divide $s(y_0 - y')$, então $r|(y_0 - y')$ e portanto $y_0 - y' = rt$ para algum $t \in \mathbf{Z}$. Donde

$$y' = y_0 - rt = y_0 - \frac{a}{d}t$$

Observando agora que

$$r(x' - x_0) = s(y_0 - y') = srt$$

obtém-se

$$x' = x_0 + st = x_0 + \frac{b}{d}t$$

Por outro lado não há dificuldade nenhuma em se verificar que, para todo $t \in \mathbf{Z}$, o par

$$\left(x_0 + \frac{b}{d}t,\ y_0 - \frac{a}{d}t\right)$$

é solução da equação dada. Isto conclui a demonstração. ■

COROLÁRIO Se a e b não são nulos e $\text{mdc}(a, b) = 1$, então a equação diofantina $ax + by = c$ tem conjunto solução não vazio dado por

$$S = \{(x_0 + bt, y_0 - at) | t \in \mathbf{Z}\}$$

onde (x_0, y_0) é uma de suas soluções particulares.

Exemplo 5: Vejamos como achar as soluções de $172x + 20y = 1\,000$. É claro que essa equação é equivalente a $43x + 5y = 250$, obtida pela divisão de seus coeficientes por 4. Como $\text{mdc}(43, 5) = 1$, esta última equação é *compatível* (tem soluções), o mesmo ocorrendo, portanto, com a equação dada. Notemos que se (x_0, y_0) é solução de $43x + 5y = 1$, então o par $(250x_0, 250y_0)$ é solução de $43x + 5y = 250$. Mas uma solução de $43x + 5y = 1$ pode ser achada conforme o exemplo 4: de

$$\begin{aligned} 43 &= 5 \cdot 8 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

obtém-se

$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) = 3 \cdot 2 + 5 \cdot (-1) = (43 - 5 \cdot 8) \cdot 2 + 5 \cdot (-1) = 43 \cdot 2 + 5 \cdot (-17)$ e portanto:

$$(x_0, y_0) = (2, -17)$$

Logo $(250x_0, 250y_0) = (500, -4\,250)$ é uma solução particular da equação dada. Conseqüentemente sua solução geral se expressa por:

$$\begin{aligned} x &= 500 + 5t \\ y &= -4\,250 - 43t \end{aligned}$$

onde $t \in \mathbf{Z}$.

Nota: Quando os coeficientes de x e y numa equação diofantina linear não são ambos positivos, sua resolução pode ser feita mais facilmente observando que: se (x_0, y_0) é solução de $ax + by = c$, então $(-x_0, y_0)$, $(x_0, -y_0)$ e $(-x_0, -y_0)$ são soluções respectivamente de

$$-ax + by = c, \quad ax - by = c \quad \text{e} \quad -ax - by = c$$

7.1 Equações diofantinas a três incógnitas

Consideremos agora a equação $a_1x + a_2y + a_3z = b$, onde os $a_i (i = 1, 2, 3)$ não são nulos. A mesma argumentação usada para provar a proposição 11 garante que essa equação admite soluções se, e somente se, $d = \text{mdc}(a_1, a_2, a_3)$ divide b.

Se $\text{mdc}(a_1, a_2) = d_1$, então existem $k_1, k_2 \in \mathbf{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. E como $d = \text{mdc}(d_1, a_3)$, então existem $k, z_0 \in \mathbf{Z}$ de maneira que $d = d_1k + a_3z_0$. Logo:

$$d = (a_1k_1 + a_2k_2)k + a_3z_0 = a_1(k_1k) + a_2(k_2k) + a_3z_0$$

Fazendo $k_1k = x_0$ e $k_2k = y_0$, então:

$$a_1x_0 + a_2y_0 + a_3z_0 = d$$

Assim, se $a_1x + a_2y + a_3z = b$ admite solução, como $b = dq$, para algum $q \in \mathbf{Z}$, então:

$$a_1(x_0q) + a_2(y_0q) + a_3(z_0q) = dq = b$$

o que mostra que (x_0q, y_0q, z_0q) é uma de suas soluções particulares.

Exemplo 6: Vejamos como encontrar uma solução particular de

$$100x + 72y + 90z = 6$$

Como mdc(100, 72, 90) = 2 e $2|6$, então essa equação é compatível. Consideremos sua forma equivalente:

$$50x + 36y + 45z = 3$$

De

$$\begin{aligned} 50 &= 36 \cdot 1 + 14 \\ 36 &= 14 \cdot 2 + 8 \\ 14 &= 8 \cdot 1 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 \end{aligned}$$

segue:

$$2 = 8 - 6 \cdot 1 = 8 - (14 - 8 \cdot 1) \cdot 1 = 8 \cdot 2 + 14 \cdot (-1) =$$
$$= (36 - 14 \cdot 2) \cdot 2 + 14 \cdot (-1) = 14(-5) + 36 \cdot 2 =$$
$$= (50 - 36 \cdot 1) \cdot (-5) + 36 \cdot 2 = 50 \cdot (-5) + 36 \cdot 7$$

Além disso:

$$45 = 2 \cdot 22 + 1 \Rightarrow 1 = 45 \cdot 1 + 2 \cdot (-22)$$

Donde:

$$1 = 45 \cdot 1 + [50 \cdot (-5) + 36 \cdot 7] \cdot (-22) =$$
$$= 50 \cdot 110 + 36 \cdot (-154) + 45 \cdot 1$$

Logo o terno (330, −462, 3) é uma solução da equação dada.

EXERCÍCIOS

250. Resolva cada uma das seguintes equações diofantinas:

a) $3x + 4y = 20$
b) $5x - 2y = 2$
c) $24x + 138y = 18$
d) $18x - 20y = -8$
e) $-26x + 39y = 65$
f) $12x - 27y = 33$

251. Dividir 100 em duas parcelas positivas tais que uma é múltiplo de 7 e a outra de 11 (Euler).

252. Ache todos os inteiros estritamente positivos com a seguinte propriedade: fornecem resto 6 quando divididos por 11 e resto 3 quando divididos por 7.

Resolução: Indiquemos por n, genericamente, esses números. Então $n = 11x + 6 = 7y + 3$. Daí $11x - 7y = -3$. Uma solução particular desta equação é $(-6, -9)$ e portanto sua solução geral é dada por $x = -6 - 7t$, $y = -9 - 11t$ $(t \in \mathbb{Z})$. Devemos impor que $n = 11(-6 - 7t) + 6 = -60 - 77t > 0$, o que leva a $t = -1, -2, -3, \ldots$ e daí $x = 1, 8, 15, \ldots$. Logo, $n = 17, 94, 171, \ldots, 77r + 17, \ldots$

253. Um parque de diversões cobra US$ 1 a entrada de crianças e US$ 3 a de adultos. Para que a arrecadação de um dia seja US$ 200, qual o menor número de pessoas, entre adultos e crianças, que poderiam freqüentar o parque nesse dia? Quantas crianças? Quantos adultos?

254. Um certo número de "seis" e de "noves" são adicionados e a soma resultante é 126. Se o número de "seis" e o de "noves" fossem permutados, a soma seria 114. Quantos "seis" e quantos "noves" foram somados?

255. Ao descontár um cheque de viagem o caixa se enganou, de maneira que recebi tantas notas de US$ 50 quanto as de US$ 10 que deveria ter recebido e vice-versa. Só depois percebi o erro e verifiquei que, se gastasse US$ 300 da importância recebida, ainda ficaria com o dobro do valor de meu cheque. Verifiquei também que este valor era o menor possível para que tal fato pudesse ocorrer. Qual a importância do cheque e quantas notas de cada espécie deveria eu ter recebido?

256. a) Resolva a equação diofantina $7x + 19y = 1\,921$.
b) Determine em $\mathbb{N} \times \mathbb{N}$ a solução (x_0, y_0) cuja soma $x_0 + y_0$ seja a menor possível.

257. Um fazendeiro que dispõe de US$ 1 770 pretende gastar essa importância na compra de cavalos e bois. Se cada cavalo custa US$ 31 e cada boi US$ 21, qual o maior número de animais que pode adquirir? Quantos cavalos? Quantos bois?

258. Uma certa quantidade de maçãs é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma quantidade. Quantas maçãs foram colocadas em cada caixa? Quantas tinha cada monte?

259. Determine o número de soluções (x_0, y_0), com $x_0 > 0$ e $y_0 > 0$, para cada uma das equações:

a) $10x + 28y = 1\,240$
b) $1\,000x - 761y = 7$

260. Encontre uma solução para cada uma das equações diofantinas:

a) $3x + 5y + 6z = 4$ c) $31x + 49y - 22z = 2$

b) $100x + 72y + 90z = 11$ d) $120x + 84y + 144z = 60$

261. Dê uma interpretação geométrica, em termos de coordenadas cartesianas, para o fato de que uma equação diofantina linear em duas incógnitas quando admite uma solução, admite infinitas.

8. Congruências

O conceito de congruência, bem como a notação através da qual se torna um dos instrumentos mais fortes da teoria dos números, foi introduzido por Karl Friedrich Gauss (1777-1855) em sua *Disquisitiones Arithmeticae* de 1801.

A título de motivação, consideremos a seguinte questão: se hoje é sábado, daqui a 152 dias, que dia da semana será? E há 152 dias, que dia da semana foi?

Consideremos a seguinte correspondência biunívoca entre a sucessão dos dias e o conjunto dos números inteiros: ao dia de hoje (sábado) associamos o número 0, ao dia de amanhã o 1, e assim por diante; ao dia de ontem (sexta-feira) associamos o -1, ao de anteontem o -2, etc. Observemos o quadro:

−14	−13	−12	−11	−10	−9	−8
−7	−6	−5	−4	−3	−2	−1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

Sua primeira coluna representa sábados: abaixo da linha do 0, posteriores a hoje; acima, anteriores. A segunda representa domingos, e assim por diante. Notemos que dois inteiros representam o mesmo dia da semana se, e somente se, sua diferença é um múltiplo de 7.

Mas na primeira coluna estão os números da forma $7k$, na segunda os da forma $7k + 1$, etc., onde $k = 0, \pm 1, \pm 2, \ldots$. Como

$$152 = 7 \cdot 21 + 5$$

então 152 está na coluna do 5, ou seja, das quintas-feiras. Logo a resposta à primeira pergunta é quinta-feira.

E como

$$-152 = 7 \cdot (-22) + 2$$

então -152 está na coluna do 2. Assim, a resposta à segunda pergunta é segunda-feira.

A definição a seguir é sugerida por questões como essa.

DEFINIÇÃO 6 Sejam a, b e m números inteiros, $m > 0$. Dizemos que a *é côngruo a* b, módulo m, se $m \mid (a - b)$. Notação: $a \equiv b \pmod{m}$.

Por exemplo: $7 \equiv 15 \pmod{8}$, pois $8 \mid (-8)$; $3 \equiv 21 \pmod{6}$, uma vez que $3 - 21 = -18$ é divisível por 6; $a \equiv a \pmod{m}$, $\forall a \in \mathbb{Z}$ e $\forall m > 0$, já que $a - a = 0$ e $m \mid 0$.

A definição 6 estabelece uma relação sobre $\mathbb{Z}$, chamada *congruência*, para a qual valem as propriedades a seguir:

$\mathbf{C_1}$ Para todo $m > 0$, a relação $\equiv$ é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência:

a $a \in \mathbb{Z} \Rightarrow a \equiv a \pmod{m}$

b $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

c $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Prova de **c**: por hipótese $m \mid (a - b)$ e $m \mid (b - c)$. Então, por $\mathbf{d_4}$ (cap. III, 6.1):

$$m \mid [(a - b) + (b - c)]$$

ou seja, $m \mid (a - c)$. Donde $a \equiv c \pmod{m}$. ■

Nota: Em virtude de $\mathbf{c_1}$, sempre que $a \equiv b \pmod{m}$ pode-se dizer que a e b são *côngruos entre si* (ou *côngruos*, apenas), módulo m. Se a e b não são côngruos entre si, diremos que são *incôngruos* módulo m e escreveremos $a \not\equiv b \pmod{m}$.

$\mathbf{C_2}$ Para quaisquer $a, b \in \mathbb{Z}$: $a \equiv b \pmod{m}$ se, e somente se, a e b fornecem mesmo resto na divisão euclidiana por m.

Prova:

$(\Rightarrow)$ Por hipótese $a = b + km$, para algum $k \in \mathbb{Z}$. Supondo que a divisão euclidiana de b por m se expresse por $b = mq + r$ $(0 \leqslant r < m)$, então

$$a = b + km = mq + r + km = m(k + q) + r$$

Como $0 \leqslant r < m$, então r é o resto na divisão euclidiana de a por m.

$(\Leftarrow)$ Se $a = mq_1 + r$ e $b = mq_2 + r$ $(0 \leqslant r < m)$, então

$$a - b = mq_1 - mq_2 = m(q_1 - q_2)$$

o que implica

$$a \equiv b \pmod{m}$$ ■

C_3 Se $a \equiv b \pmod m$, então $a \pm c \equiv b \pm c \pmod m$ e $ac \equiv bc \pmod m$, para todo $c \in \mathbb{Z}$.

Prova da segunda afirmação: por hipótese $a - b = mq$, $q \in \mathbb{Z}$. Logo $ac - bc = m(qc)$ e isto significa que $ac \equiv bc \pmod m$. ■

C_4 Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $a \pm c \equiv b \pm d \pmod m$ e $ac \equiv bd \pmod m$.

Prova da segunda afirmação: das hipóteses e de c_3 decorre que $ac \equiv bc \pmod m$ e $cb \equiv db \pmod m$. Logo, pela transitividade: $ac \equiv bd \pmod m$.

Isto posto, por indução se mostra que: para quaisquer $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, se $a_i \equiv b_i \pmod m$, então:

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m \quad \text{e} \quad \prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod m.$$

Em particular vale a

C_5 Se $a \equiv b \pmod m$, então $ra \equiv rb \pmod m$ e $a^r \equiv b^r \pmod m$, para todo inteiro $r \geqslant 1$. ■

Exemplo 7: Mostremos que $10^{200} - 1$ é divisível por 11. Como $10 \equiv -1 \pmod{11}$, então $10^{200} \equiv (-1)^{200} \equiv 1 \pmod{11}$. Portanto $10^{200} - 1 \equiv 0 \pmod{11}$ e daí se conclui que:

$$11 \mid (10^{200} - 1)$$

C_6 Se $ca \equiv cb \pmod m$ e $\text{mdc}(m, c) = d > 0$, então:

$$a \equiv b \left(\text{mod } \frac{m}{d}\right)$$

Prova: Por hipótese $c(a - b) = mk$, para algum $k \in \mathbb{Z}$. Daí:

$$\frac{c}{d}(a - b) = \frac{m}{d}k$$

onde $\text{mdc}\left(\frac{c}{d}, \frac{m}{d}\right) = 1$. Donde $\frac{m}{d} \mid (a - b)$ e portanto $a \equiv b \left(\text{mod } \frac{m}{d}\right)$.

COROLÁRIO 1 Se $ca \equiv cb \pmod m$ e $\text{mdc}(c, m) = 1$, então $a \equiv b \pmod m$.

COROLÁRIO 2 Se $ca \equiv cb \pmod p$, onde p é primo e $p \nmid c$, então $a \equiv b \pmod p$.

8.1 Sistemas completos de restos

Sendo a congruência uma relação de equivalência sobre $\mathbb{Z}$, então, para todo $m > 0$, fica determinada sobre o conjunto dos inteiros, através de $\equiv$, uma partição em classes de equivalência, módulo m.

Por exemplo, se $m = 3$, as classes são:

$\{\ldots, -9, -6, -3, 0, +3, +6, +9, \ldots\}$
$\{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$
$\{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

onde dois elementos de uma mesma classe são côngruos entre si, módulo 3, e dois elementos quaisquer, de classes distintas, são incôngruos, módulo 3.

A escolha conveniente de um elemento em cada uma das classes, para representá-la, muitas vezes pode facilitar o trabalho com questões que envolvem congruências. Daí a definição a seguir.

DEFINIÇÃO 7 Um conjunto de m inteiros, $m > 0$, forma um *sistema completo de restos módulo m* se dois quaisquer desses números, diferentes entre si, são incôngruos módulo m.

Exemplo 8: O conjunto $\{0, 1, 2, \ldots, m - 1\}$ é um sistema completo de restos módulo m. De fato, se i e j são inteiros tais que $0 \leqslant i < j < m$, então $0 < j - i < m$ e portanto $j \not\equiv i \pmod m$. Esse conjunto é chamado *sistema completo de restos mínimos positivos*.

PROPOSIÇÃO 13 Se $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de restos módulo m, então todo inteiro a é côngruo a um e somente um dos r_i.

Demonstração: Aplicando o algoritmo da divisão aos elementos a e m: $a = mq + r$, onde $0 \leqslant r < m$. Ou seja: $a \equiv r \pmod m$, onde $r \in \{0, 1, \ldots, m - 1\}$. Por outro lado, como conseqüência de C_2, a divisão de $r_1, r_2, \ldots, r_m$ por m fornecerá m restos, distintos dois a dois, e daí, para um certo r_j, obter-se-á:

$$r_j = mq_j + r$$

ou

$$r_j \equiv r \pmod m$$

Como $a \equiv r \pmod m$, então $a \equiv r_j \pmod m$.

E se $a \equiv r_k \pmod m$, então $r_j \equiv r_k \pmod m$, o que implica $r_j = r_k$, pela definição de sistema completo de restos. ■

Exemplo 9: Se m é ímpar, o conjunto formado pelos inteiros

$$0, \pm 1, \pm 2, \ldots, \pm \frac{m-1}{2}$$

é um sistema completo de restos. Com efeito, tomando i e j dentre esses elementos, com $i \neq j$, então:

$$|i| \leqslant \frac{m-1}{2} \text{ e } |j| \leqslant \frac{m-1}{2}$$

Daí:

$$0 < |i-j| \leqslant |i| + |j| \leqslant m - 1 < m$$

Logo, $i \not\equiv j \pmod{m}$.

Deixamos como exercício a prova de que se m é par, então:

$$\left\{0, \pm 1, \ldots, \pm\left(\frac{m}{2} - 1\right), \frac{m}{2}\right\}$$

é um sistema completo de restos módulo m.

Exemplo 10: Mostremos que a congruência $x^2 + 1 \equiv 0 \pmod{8}$ não tem soluções. Usando o sistema de restos apontado por último, ou seja, $\{0, \pm 1, \pm 2, \pm 3, 4\}$, então pode-se dizer que todo $x \in \mathbb{Z}$ é côngruo a um apenas dos elementos desse conjunto. Em resumo:

$$x \equiv 0, \pm 1, \pm 2, \pm 3, 4 \pmod{8} \quad (*)$$

Então:

$$x^2 \equiv 0, 1, 4, 9, 16 \pmod{8}$$

ou

$$x^2 \equiv 0, 1, 4 \pmod{8}$$

já que $9 \equiv 1 \pmod{8}$ e $16 \equiv 0 \pmod{8}$. Daí

$$x^2 + 1 \equiv 1, 2, 5 \pmod{8}, \ \forall x \in \mathbb{Z},$$

o que garante nossa afirmação.

Exemplo 11 (critério de divisibilidade por 11):

Seja $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$ um número de nosso sistema de numeração (conforme cap. II, item 5). Como $10 \equiv -1 \pmod{11}$, então $10^s \equiv -1 \pmod{11}$ se n é ímpar e $10^s \equiv 1 \pmod{11}$ se n é par. Assim:

(*) $x \equiv 0$ ou $x \equiv +1$ ou $x \equiv -1$, etc., "ou" exclusivo.

$$\begin{aligned} a_0 &\equiv a_0 \pmod{11} \\ 10 \cdot a_1 &\equiv -a_1 \pmod{11} \\ 10^2 \cdot a_2 &\equiv a_2 \pmod{11} \\ &\vdots \\ 10^r \cdot a_r &\equiv (-1)^r a_r \pmod{11} \end{aligned}$$

Logo:

$$n = a_0 + 10a_1 + \ldots + 10^r a_r \equiv a_0 - a_1 + a_2 - \ldots + (-1)^r a_r \pmod{11}$$

Como, por $\mathbf{C_2}$, n e $a_0 - a_1 + a_2 - \ldots + (-1)^r a_r$ fornecem o mesmo resto na divisão por 11, então pode-se afirmar que: "n é divisível por 11 se, e somente se, $a_0 - a_1 + a_2 - \ldots + (-1)^r a_r$ é divisível por 11.

Assim, o número 7 568 é divisível por 11 pois $8 - 6 + 5 - 7$ é divisível por 11.

Exemplo 12 (*prova dos noves*)

A chamada *prova dos noves* é baseada, em princípio, no fato de que:

$$a = b \pm c \Rightarrow a \equiv b \pm c \pmod{9}$$

$$a = bc \Rightarrow a \equiv bc \pmod{9}$$

Como essas implicações não valem em sentido contrário, então essa prova pode detectar se há erros num cálculo — mas não garante que este esteja necessariamente certo. A escolha do "nove", por outro lado, é apenas uma conveniência decorrente de nosso sistema de numeração. De fato, se a representação polinomial decimal de um inteiro $n > 0$ é

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r \quad (0 \leqslant a_i \leqslant 9)$$

então

$$n \equiv a_0 + a_1 + \ldots + a_r \pmod{9}$$

pois o fato de que $10 \equiv 1 \pmod{9}$ implica $10^k \equiv 1 \pmod{9}$, para todo $k \geqslant 1$. Assim, n e $a_0 + a_1 + \ldots + a_r$ têm o mesmo resto na divisão euclidiana por 9. Então é bastante cômodo achar o resto da divisão de n por 9 — daí a escolha desse número para a prova.

Por exemplo, suponhamos que na divisão de $a = 1\,284\,125$ por $b = 3\,768$ tivéssemos achado $q = 340$ (quociente) e $r = 3\,005$ (resto). Como devemos ter $a = bq + r$, então $a \equiv bq + r \pmod{9}$. Para cada um desses inteiros, "noves fora", obtemos: $a \equiv 1 + 2 + 8 + 4 + 1 + 2 + 5 \equiv 5 \pmod{9}$, $b \equiv 3 + 7 + 6 + 8 \equiv 6 \pmod{9}$, $q \equiv 3 + 4 + 0 \equiv 7 \pmod{9}$ e $r \equiv 3 + 0 + 0 + 5 \equiv 8 \pmod{9}$.

Então:

$$bq + r \equiv 6 \cdot 7 + 8 \equiv 50 \equiv 5 \equiv a \pmod{9}$$

Assim, a divisão feita passou pela prova dos noves.

EXERCÍCIOS

262. Ache todos os inteiros x tais que:

a) $0 \leqslant x \leqslant 100$ e $x \equiv 5 \pmod 8$
b) $100 \leqslant x \leqslant 200$ e $x \equiv -1 \pmod 7$

263. Se $402 \equiv 654 \pmod m$, ache os possíveis valores de m.

264. Ache os restos nas seguintes divisões:

a) 2^{45} por 7
b) 11^{10} por 100
c) $3^{10} \cdot 42^5 + 6^8$ por 5
d) $5^2 \cdot 4\,841 + 28^5$ por 3
e) 11^{69} por 3

Resolução de c): Como $3 \equiv -2 \pmod 5$, então $3^2 \equiv 4 \equiv -1 \pmod 5$; daí $3^4 \equiv 1 \pmod 5$ e portanto $3^8 \equiv 1 \pmod 5$; logo $3^{10} \equiv (-1) \cdot 1 \pmod 5$; como $-1 \equiv 4 \pmod 5$, então $3^{10} \equiv 4 \pmod 5$. Observando que $42 \equiv 2 \pmod 5$, então $42^2 \equiv 4 \equiv -1 \pmod 5$ e daí $42^4 \equiv 1 \pmod 5$; donde $42^5 \equiv 2 \cdot 1 \equiv 2 \pmod 5$. Obviamente $6^8 \equiv 1 \pmod 5$, pois $6 \equiv 1 \pmod 5$. Assim

$$3^{10} \cdot 42^5 + 6^8 \equiv 4 \cdot 2 + 1 \equiv 4 \pmod 5$$

Pela propriedade $\mathbf{C_2}$ o resto é 4.

265. Mostre que $2^{20} - 1$ é divisível por 41.

266. Qual o resto na divisão euclidiana de $s = 1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$ por 4? Justifique.

267. Mostre que o resto na divisão euclidiana de $s(n) = 1! + 2! + 3! + \ldots + n!$ por 12 é 9, para todo $n \geqslant 4$.

Sugestão: Se $n \geqslant 4$, então $n! \equiv 0 \pmod{12}$.

268. Se n é um múltiplo de 4, qual o resto da divisão de

$$1^n + 2^n + \ldots + 8^n + 9^n$$

por 10?

269. a) Mostre que o resto da divisão de um número inteiro positivo por 10 é seu algarismo das unidades.
b) Mostre que o resto da divisão de um inteiro positivo por 100 é o número formado por seus dois últimos algarismos.

Sugestão: Considerar o número na forma

$$a_0 + a_1 \cdot 10 + \ldots + a_r \cdot 10^r$$

270. Ache o algarismo das unidades dos seguintes números: $7^{(7^7)}$ e $9^{(9^9)}$.

Resolução: Como $7 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$ e $7^4 \equiv 1 \pmod{10}$, então $7^r \equiv 7, 9, 3$ ou $1 \pmod{10}$, conforme, respectivamente, $r \equiv 1, 2, 3$ ou $0 \pmod 4$. Mas $7 \equiv 3 \pmod 4$, $7^2 \equiv 1 \pmod 4$, $7^3 \equiv 3 \pmod 4$, $7^4 \equiv 1 \pmod 4$, ... Ou seja, $7^s \equiv 3$ ou $1 \pmod 4$, conforme s seja ímpar ou par. Como 7^7 é ímpar, então $7^7 \equiv 3 \pmod 4$. Logo $7^{(7^7)} \equiv 3 \pmod{10}$. Assim, o algarismo das unidades do número dado é 3.

271. Se $a \equiv b \pmod m$ e $n \mid m$ $(n > 1)$, mostre que $a \equiv b \pmod n$.

272. Ache os dois últimos algarismos do número

$$n = 7^{(7^{1000})}$$

273. Se $a \equiv b \pmod{m_1}$ e $a \equiv b \pmod{m_2}$, mostre que $a \equiv b \pmod m$, onde $m = \text{mmc}(m_1, m_2)$. (Assim, se $\text{mdc}(m_1, m_2) = 1$, então $a \equiv b \pmod{m_1 m_2}$.)

274. Se $a \equiv b \pmod m$, prove que:

$$\text{mdc}(a, m) = \text{mdc}(b, m)$$

275. Mostre que o algarismo das unidades do número $s = 1^n + 2^n + 3^n + 4^n$ é 4 se $n \equiv 0 \pmod 4$ e é 0 nos demais casos, para todo $n \in \mathbb{N}^*$.

Resolução: No caso $n \equiv 0 \pmod 4$ valem as congruências $1^n \equiv 1 \pmod{10}$, $2^n \equiv 6 \pmod{10}$, $3^n \equiv 1 \pmod{10}$ e $4^n \equiv 6 \pmod{10}$, o que implica $s \equiv 1 + 6 + 1 + 6 \equiv 4 \pmod{10}$. Se $n \equiv 1 \pmod 4$, então $1^n \equiv 1 \pmod{10}$, $2^n \equiv 2 \pmod{10}$, $3^n \equiv 3 \pmod{10}$ e $4^n \equiv 4 \pmod{10}$ e portanto $s \equiv 1 + 2 + 3 + 4 \equiv 10 \equiv 0 \pmod{10}$. O raciocínio é o mesmo para os dois casos restantes.

276. Mostre que $0, 1, 2, 2^2, \ldots, 2^9$ formam um sistema completo de restos, módulo 11, mas que o mesmo não acontece com $0, 1^2, 2^2, 3^2, \ldots, 10^2$.

277. Seja $m > 1$ um inteiro. Se $a \in \mathbb{Z}$ e $\text{mdc}(a, m) = 1$, prove que

$$c, c + a, c + 2a, \ldots, c + (m - 1)a$$

formam um sistema completo de restos módulo m, para qualquer inteiro c.

278. Se $r_1, r_2, \ldots, r_m$ formam um sistema completo de restos módulo m, mostre que o mesmo se pode dizer de

$$r_1 + a, r_2 + a, \ldots, r_m + a$$

para todo $a \in \mathbb{Z}$.

279. Se $n > 0$ não é múltiplo de 3, prove que $a = 3^{2n} + 3^n + 1$ é divisível por 13.

Resolução: Como $3 \equiv 3 \pmod{13}$, $3^2 \equiv 9 \pmod{13}$, $3^3 \equiv 1 \pmod{13}$, $3^4 \equiv 3 \pmod{13}$, ..., então $3^{3t+1} \equiv 3 \pmod{13}$ e $3^{3t+2} \equiv 9 \pmod{13}$.

Além disso: $9 \equiv 9 \pmod{13}$, $9^2 \equiv 81 \equiv 3 \pmod{13}$, $9^3 \equiv 27 \equiv 1 \pmod{13}$, $9^4 \equiv 9 \pmod{13}$, ... Ou seja:

$$9^{3t+1} \equiv 9 \pmod{13} \text{ e } 9^{3t+2} \equiv 3 \pmod{13}$$

Assim, para $n = 3t + 1$:

$$a = 9^n + 3^n + 1 \equiv 9 + 3 + 1 \equiv 0 \pmod{13}$$

Analogamente se procede para $n = 3t + 2$.

280. Use sistemas de restos convenientes para provar que:

a) Se a é ímpar, $a^2 \equiv 1 \pmod 8$.
b) Para todo inteiro a, $a^3 \equiv 0$, 1 ou 8 (mod 9).
c) Para todo inteiro a, $a^3 \equiv a \pmod 6$.
d) Se a é um inteiro, $2 \nmid a$ e $3 \nmid a$, então $a^2 \equiv 1 \pmod{24}$.
e) Se a é *quadrado perfeito* ($a = t^2$, $t \in \mathbb{Z}$) e também *cubo perfeito* ($a = s^3$, $s \in \mathbb{Z}$), então $a \equiv 0$, 1, 9 ou 28 (mod 36).
f) Se a é cubo perfeito, $a \equiv 0$, 1 ou -1 (mod 9).

Resolução de f): Vamos supor $a = t^3$. Como $t \equiv 0, \pm1, \pm2, \pm3, \pm4 \pmod 9$, então $t^3 \equiv 0, \pm1, \pm8, \pm27, \pm64 \pmod 9$. Mas $8 \equiv -1 \pmod 9$, $-8 \equiv 1 \pmod 9$, $27 \equiv 0 \pmod 9$, $-27 \equiv 0 \pmod 9$, $64 \equiv 1 \pmod 9$ e $-64 \equiv -1 \pmod 9$. Logo $a = t^3 \equiv 0$, 1 ou -1 (mod 9).

281. Mostre que, para todo inteiro a: a) o algarismo das unidades de a^2 é 0, 1, 4, 5, 6 ou 9. b) o algarismo das unidades de a^3 pode ser qualquer dos algarismos de nosso sistema de numeração. c) o algarismo das unidades de a^4 é 0, 1, 5 ou 6.

282. Mostre que os inteiros 1 111, 111 111, 11 111 111, ... (número de algarismos par), são todos números compostos.

283. Seja $a_r a_{r-1} \ldots a_2 a_1 a_0$ a representação decimal em nosso sistema de numeração de um inteiro positivo n (portanto $0 \leqslant a_i \leqslant 9$, $i = 0, 1, 2, \ldots, r$). Prove que n é divisível por 7 se, e somente se,

$$a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \ldots$$

é divisível por 7.

284. Estabeleça critérios de divisibilidade por 4, por 5 e por 6.

285. Seja a um inteiro positivo e indiquemos por b o inteiro formado quando se escrevem os algarismos de a na ordem contrária. (Por exemplo, se a = 1 236, b = 6 321.) Prove que $a \equiv b \pmod 9$ e portanto $9 \mid (a - b)$.

286. Um *palíndromo* é um número que, escrito da direita para a esquerda ou da esquerda para a direita, o resultado é o mesmo. (Por exemplo, 373 e 52 125 são palíndromos.) Prove que todo palíndromo com um número par de algarismos é divisível por 11.

287. Seja $a_r a_{r-1} \ldots a_2 a_1 a_0$ a representação decimal de um número natural n e consideremos $k \in \mathbb{N}$, $1 \leqslant k \leqslant r$. Prove que n é divisível por 2^k se, e somente se, o número $a_{k-1} a_{k-2} \ldots a_1 a_0$ é divisível por 2^k.

Resolução: Observemos que:

$$n = a_r \cdot 10^r + \ldots + a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$$

Como $10^k \equiv 0 \pmod{2^k}$, $10^{k+1} \equiv 0 \pmod{2^k}$, ..., $10^r \equiv 0 \pmod{2^k}$, então:

$$n \equiv a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \pmod{2^k}$$

Ou seja:

$$n \equiv a_{k-1} a_{k-2} \ldots a_1 a_0 \pmod{2^k}$$

Logo: $2^k \mid n \iff 2^k \mid a_{k-1} a_{k-2} \ldots a_1 a_0$

Em particular, n é divisível por 4 se $a_1 a_0$ (número formado pelos dois últimos algarismos de n) é divisível por 4, por 8 se $a_2 a_1 a_0$ é divisível por 8, etc.

288. Aplique os critérios de divisibilidade para verificar se:

a) 125 431 784 é divisível por 7.
b) 4 × (373 112) é divisível por 16.
c) 1 978 542 é divisível por 77.
d) 2 810 542 é divisível por 18.
e) (3 145) × (253) × 9^9 é divisível por 11.

289. Mostre que $10^{3k} \equiv 1 \pmod{1\,001}$ se k é um número natural par e que $10^{3k} \equiv -1 \pmod{1\,001}$ se k é ímpar.

290. Se o número x679y (x e y representam algarismos) é divisível por 72, ache x e y.

291. Sem efetuar os cálculos, aplique a prova dos noves aos seguintes exemplos:

a) $65 + 101 + 1\,213 + 48 = 1\,427$

b)
```
      6 4 2
    × 2 1 5
    -------
    • • • •
    • • •
  • • • •
  ---------
  1 3 0 8 3 0
```

c)
```
1 4 8 2 4 5 | 1 2 1
  • • •     |---------
    • • •     1 2 2 5
      • • •
        3 0
```

Qual a conclusão, em cada caso?

9. Congruências lineares

DEFINIÇÃO 8 Uma congruência algébrica do tipo

$$ax \equiv b \pmod{m}$$

onde $a, b, m \in \mathbf{Z}$, $a \neq 0$ e $m > 0$, e x é uma variável em $\mathbf{Z}$, recebe o nome de *congruência linear* ou *congruência de primeiro grau*.

Seja u uma solução de $ax \equiv b \pmod{m}$, ou seja, u é um inteiro tal que $au \equiv b \pmod{m}$. Aplicando o algoritmo da divisão para u e m:

$$u = mq + x_0 \; (0 \leqslant x_0 < m)$$

Assim $au = amq + ax_0$, e como $m \equiv 0 \pmod{m}$ e portanto $amq \equiv 0 \pmod{m}$, então $ax_0 \equiv au \pmod{m}$. Daí:

$$ax_0 \equiv b \pmod{m}$$

o que mostra que x_0 também é solução da congruência considerada. Convencionaremos que todos os $x \in Z$ tais que $x \equiv x_0 \pmod{m}$ constituem uma única solução de $ax \equiv b \pmod{m}$.

Por exemplo, como 4 é solução de $2x \equiv 3 \pmod{5}$, então todos os elementos de $\{4 + 5t \mid t \in \mathbf{Z}\} = \{4, -1, 9, -6, \ldots\}$ são apenas representações da mesma solução.

PROPOSIÇÃO 14 Uma congruência linear $ax \equiv b \pmod{m}$, onde $a \neq 0$, admite soluções em $\mathbf{Z}$ se, e somente se, b é divisível por $d = \text{mdc}(a, m)$. E, neste caso, se x_0 é uma solução particular, então o conjunto de todas as soluções tem d elementos, a saber:

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\,\frac{m}{d},\ \ldots,\ x_0 + (d-1)\,\frac{m}{d}$$

Demonstração: Seja x_0 uma solução de $ax \equiv b \pmod{m}$. Então $ax_0 - my_0 = b$, para algum $y_0 \in \mathbf{Z}$. Logo (x_0, y_0) é solução de $ax - my = b$. Da mesma forma, se (x_0, y_0) é solução de $ax - my = b$, então x_0 é solução de $ax \equiv b \pmod{m}$. Como a condição de existência de soluções para $ax - my = b$, devido à proposição 11, é que b seja divisível por d = mdc (a, m), o mesmo vale para $ax \equiv b \pmod{m}$.

Lembremos ainda que se (x_0, y_0) é solução de $ax - my = b$, então:

$$x = x_0 + \frac{m}{d}t \qquad \text{e} \qquad y = y_0 + \frac{a}{d}t$$

$t \in \mathbf{Z}$, fornecem todas as soluções. Logo a solução genérica de $ax \equiv b \pmod{m}$ é dada por:

$$x = x_0 + \frac{m}{d}t \quad (t \in \mathbf{Z})$$

Aplicando o algoritmo da divisão para t e d: $t = dq + r \; (0 \leqslant r < d)$. Assim:

$$x = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(dq + r) = x_0 + \frac{m}{d}r + mq \equiv x_0 + \frac{m}{d}r \pmod{m}$$

ou seja, x está entre as soluções apontadas no enunciado.

Por outro lado, supondo

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}$$

onde $0 \leqslant t_1 < t_2 < d$, então:

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m}$$

e como mdc $\left(\frac{m}{d}, m\right) = \frac{m}{d}$, a propriedade $\mathbf{C}_6$ leva a concluir que

$$t_1 \equiv t_2 \pmod d$$

o que é impossível.

Assim as soluções do enunciado, sendo incôngruas módulo m, são todas as soluções de $ax \equiv b \pmod m$, conforme convenção feita após a definição 8. ■

Exemplo 13: Se em $ax \equiv b \pmod m$ se tem $\text{mdc}(a, m) = 1$, então essa congruência linear só admite uma solução. É o caso de

$$3x \equiv 1 \pmod 5$$

cujo conjunto solução é $\{2\}$.

Exemplo 14: A congruência $6x \equiv 15 \pmod{21}$ admite 6 como solução particular. Logo, o conjunto de suas soluções é, já que $\text{mdc}(6, 21) = 3$: $\left\{6, 6 + \frac{21}{3}, 6 + 2 \cdot \frac{21}{3}\right\} = \{6, 13, 20\}$.

10. Sistemas de congruências

Uma vez estudadas as congruências lineares, podemos pensar agora em resolver sistemas de congruências lineares simultâneas. Tais sistemas se apresentam genericamente assim:

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_rx \equiv b_r \pmod{m_r} \end{cases}$$

onde os a_i $(i = 1, 2, \ldots, r)$ são supostos não nulos. Uma solução do sistema é um inteiro x_0 que é solução de cada uma das congruências que dele fazem parte. Assim, se uma de suas congruências não admite solução, o mesmo ocorre com o sistema.

Consideremos o seguinte exemplo:

$$\begin{cases} 3x \equiv 1 \pmod 5 \\ 2x \equiv 3 \pmod 9 \end{cases}$$

Uma das soluções da primeira congruência é 2 e uma solução particular da segunda é 6. Logo, as soluções gerais são dadas por

$$x = 2 + 5t,\ t \in \mathbb{Z} \text{ (para a primeira equação)}$$

e

$$x = 6 + 9s,\ s \in \mathbb{Z} \text{ (para a segunda)}$$

que podem ser traduzidas, em termos de congruências, por:

$$x \equiv 2 \pmod 5 \text{ e } x \equiv 6 \pmod 9$$

Como a multiplicação da primeira dessas congruências por 3 leva a $3x \equiv 1 \pmod 5$ e a multiplicação da segunda por 2 leva a $2x \equiv 3 \pmod 9$, então o sistema dado equivale a:

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 6 \pmod 9 \end{cases}$$

Daí porque, doravante, nos ateremos apenas a este tipo de sistema (coeficientes de x iguais a 1).

Aliás a resolução deste último, em se tratando de achar a intersecção dos conjuntos soluções de cada congruência do sistema, pode ser encaminhado da maneira habitual neste tipo de problema. Vejamos como:

Substituindo-se a solução geral $x = 2 + 5t$ da primeira congruência na segunda obtém-se:

$$2 + 5t \equiv 6 \pmod 9$$

que equivale a

$$5t \equiv 4 \pmod 9$$

Sendo $t_0 = 8$ uma solução particular desta última, então $t = 8 + 9k$ é sua solução geral. Assim:

$$x = 2 + 5t = 2 + 5(8 + 9k) = 42 + 45k\ (k \in \mathbb{Z})$$

ou

$$x \equiv 42 \pmod{45}$$

é a solução do sistema.

PROPOSIÇÃO 15 Um sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

admite solução se, e somente se, $a_1 - a_2$ é divisível por $d = \text{mdc}(m_1, m_2)$. Neste caso, se x_0 é uma solução particular do sistema e se $m = \text{mmc}(m_1, m_2)$, então $x \equiv x_0 \pmod m$ é sua solução geral.

Demonstração:

($\Rightarrow$) Se x_0 é solução particular do sistema, então existe $t \in \mathbf{Z}$ tal que

$$x_0 = a_1 + m_1 t \quad \text{e} \quad a_1 + m_1 t \equiv a_2 \pmod{m_2}$$

Daí:

$$m_1 t \equiv a_2 - a_1 \pmod{m_2}$$

e, pela proposição 14, $d \mid (a_2 - a_1)$.

($\Leftarrow$) Como $d \mid (a_2 - a_1)$, por hipótese, então

$$m_1 y \equiv a_2 - a_1 \pmod{m_2}$$

admite uma solução y_0. Daí

$$a_1 + m_1 y_0 \equiv a_2 \pmod{m_2}$$

Como, obviamente,

$$a_1 + m_1 y_0 \equiv a_1 \pmod{m_1}$$

então $a_1 + m_1 y_0$ é solução do sistema.

Se x_0 indica uma solução particular do sistema e x indica genericamente suas soluções, então $x_0 \equiv a_1 \pmod{m_1}$ e $x \equiv a_1 \pmod{m_1}$, do que segue

$$x \equiv x_0 \pmod{m_1}$$

ou seja: $m_1 \mid (x - x_0)$. Analogamente se chega a que $m_2 \mid (x - x_0)$. Então, $m \mid (x - x_0)$, o que pode ser traduzido por:

$$x \equiv x_0 \pmod{m}. \quad ■$$

COROLÁRIO Um sistema de congruências

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

admite soluções se, e somente se, $a_i - a_j$ é divisível por $d_{ij} = \text{mdc}(m_i, m_j)$, para qualquer par de índices i, j ($i \neq j$). Neste caso, se x_0 é uma solução particular, então a solução geral do sistema é dada por:

$$x \equiv x_0 \pmod{m}$$

onde $m = \text{mmc}(m_1, m_2, \ldots, m_r)$. ■

Exemplo 15: Consideremos o sistema

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{4} \\ x \equiv 9 \pmod{6} \end{cases}$$

É fácil verificar que ele satisfaz as condições do corolário e portanto admite soluções. Uma delas é o número 27. Como

$$\text{mmc}(5, 4, 6) = \text{mmc}(\text{mmc}(5, 4), 6) = \text{mmc}(20, 6) = 60$$

então

$$x \equiv 27 \pmod{60}$$

é a solução geral.

PROPOSIÇÃO 16 (teorema chinês do resto): Sejam $m_1, m_2, \ldots, m_r$ números inteiros maiores que zero e tais que $\text{mdc}(m_i, m_j) = 1$, sempre que $i \neq j$. Façamos $m = m_1 m_2 \ldots m_r$ e sejam $b_1, b_2, \ldots, b_r$, respectivamente, soluções das congruências lineares

$$\frac{m}{m_j} y \equiv 1 \pmod{m_j} \; (j = 1, 2, \ldots, r)$$

Então o sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

é possível (admite soluções) para quaisquer $a_1, a_2, \ldots, a_r \in \mathbf{Z}$ e sua solução geral é dada por:

$$x \equiv a_1 b_1 \frac{m}{m_1} + \ldots + a_r b_r \frac{m}{m_r} \pmod{m}$$

Demonstração: Que o sistema é possível decorre do corolário da proposição anterior.

Notemos que, como $\text{mdc}(m_j, m_i) = 1$ para $i \neq j$, então

$$\text{mdc}\left(m_j, \frac{m}{m_j}\right) = 1$$

o que implica a existência de soluções para cada congruência linear

$$\frac{m}{m_j} y \equiv 1 \pmod{m_j}$$

as quais estamos indicando por b_j ($j = 1, 2, \ldots, r$). Assim,

$$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$$

e portanto:

$$a_j b_j \frac{m}{m_j} \equiv a_j \pmod{m_j} \quad (j = 1, 2, \ldots, r).$$

Por outro lado, se $i \neq j$:

$$\frac{m}{m_i} \equiv 0 \pmod{m_j}$$

e então

$$a_i b_i \frac{m}{m_i} \equiv 0 \pmod{m_j}$$

Logo:

$$a_1 b_1 \frac{m}{m_1} + \ldots + a_j b_j \frac{m}{m_j} + \ldots + a_r b_r \frac{m}{m_r} \equiv a_j \pmod{m_j}$$

para todo j, $1 \leqslant j \leqslant r$. Assim, de fato

$$x_0 = \sum_{i=1}^{r} a_i b_i \frac{m}{m_i}$$

é uma solução particular do sistema. O corolário da proposição anterior garante então que

$$x \equiv x_0 \pmod{m}$$

é a solução geral posto que, como $\mathrm{mdc}(m_i, m_j) = 1$, sempre que $i \neq j$, então $\mathrm{mmc}(m_1, m_2, \ldots, m_r) = m_1 m_2 \ldots m_r = m$. ■

Exemplo 16: Vamos resolver o sistema

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

segundo o teorema chinês do resto. Neste caso $m = 30$ e as congruências a resolver são: $15y \equiv 1 \pmod 2$, $10y \equiv 1 \pmod 3$ e $6y \equiv 1 \pmod 5$, das quais $b_1 = 1$, $b_2 = 1$ e $b_3 = 1$ são soluções particulares. Assim, a solução geral do sistema é dada por:

$$x \equiv 1 \cdot 1 \cdot 15 + 2 \cdot 1 \cdot 10 + 3 \cdot 1 \cdot 6 \equiv 23 \pmod{30}$$

EXERCÍCIOS

292. Resolva as seguintes congruências lineares:

a) $5x \equiv 2 \pmod{26}$
b) $3x \equiv 17 \pmod 5$
c) $34x \equiv 60 \pmod{98}$
d) $6x \equiv 15 \pmod{21}$
e) $20x \equiv 7 \pmod{15}$
f) $14x \equiv 36 \pmod{48}$
g) $5x \equiv -38 \pmod 7$
h) $20x \equiv 30 \pmod{31}$

293. Resolva os seguintes sistemas de congruências simultâneas:

a) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$
b) $x \equiv 1 \pmod 9$, $x \equiv 5 \pmod 7$, $x \equiv 3 \pmod 5$
c) $3x \equiv 1 \pmod{10}$, $4x \equiv 2 \pmod 7$
d) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $2x \equiv 3 \pmod 7$
e) $2x \equiv 1 \pmod 5$, $4x \equiv 1 \pmod 7$, $5x \equiv 9 \pmod{11}$

294. Ache um inteiro x tal que $x \equiv 3 \pmod{11}$, $x \equiv 5 \pmod{19}$, $x \equiv 10 \pmod{29}$ (Euler).

295. Ache um inteiro x tal que $x \equiv 3 \pmod{10}$, $x \equiv 11 \pmod{13}$ e $x \equiv 15 \pmod{17}$ (Regiomontanus — séc. XV).

296. Ache o menor inteiro que fornece restos 1, 2, 5 e 5 quando dividido, respectivamente, por 2, 3, 6 e 12 (Yih-Hing — séc. VII).

297. Ache o menor inteiro $a > 2$ tal que: $2 | a$, $3 | (a + 1)$, $4 | (a + 2)$ e $5 | (a + 3)$.

Resolução: O problema pode ser equacionado mediante o sistema:

$$a \equiv 0 \pmod 2,\ a \equiv 2 \pmod 3,\ a \equiv 2 \pmod 4 \text{ e } a \equiv 2 \pmod 5$$

que, pelo corolário da proposição 15, admite soluções. Da primeira congruência sai $a = 2r$. Substituindo na segunda: $2r \equiv 2 \pmod 3$; donde $r = 1 + 3s$ e então $a = 2 + 6s$. Passando à terceira congruência: $2 + 6s \equiv 2 \pmod 4 \Longleftrightarrow 3s \equiv 0 \pmod 2$; daí $s = 2t$ e então $a = 2 + 12t$. Finalmente: $2 + 12t \equiv 2 \pmod 5 \Longleftrightarrow 12t \equiv 0 \pmod 5 \Longleftrightarrow t = 5k$. Assim, $a = 2 + 60k$ ($k \in \mathbb{Z}$) e a resposta é 62.

298. Retirando-se os ovos contidos num cesto 2, 3, 4, 5 e 6 de cada vez restarão, respectivamente, 1, 2, 3, 4 e 5 ovos. Quando eles são retirados de 7 em 7, não sobra nenhum no cesto. Qual o menor número de ovos que um cesto nessas condições pode conter? (Brahmagupta — séc. VII)

299. (Antigo problema chinês) Um bando de 17 piratas, ao tentar dividir entre si, igualmente, as moedas de ouro de uma arca, verifica que 3 moedas sobrariam. Na discussão que se seguiu um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita 10 moedas sobrariam. Novo qüiproquo e mais um pirata é morto. Mas agora, por fim, é possível dividir igualmente a fortuna entre eles. Qual o menor número de moedas que a arca poderia conter?

300. Resolva, mediante o teorema chinês do resto, os seguintes sistemas:

a) $\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 4 \pmod{11} \\ x \equiv 6 \pmod{13} \end{cases}$ b) $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv -1 \pmod 9 \\ x \equiv 6 \pmod{10} \end{cases}$

301. a) Mostre que o fato de $360 = 5 \cdot 8 \cdot 9$, onde os fatores são primos entre si, implica que resolver a congruência $7x \equiv 4 \pmod{360}$ equivale a resolver o sistema

$$\begin{cases} 7x \equiv 4 \pmod 5 \\ 7x \equiv 4 \pmod 8 \\ 7x \equiv 4 \pmod 9 \end{cases}$$

b) Resolva, usando o teorema chinês do resto, o sistema que aparece em a).

302. Procure três inteiros consecutivos, o primeiro dos quais é divisível por um quadrado, o segundo por um cubo e o terceiro por uma quarta potência (quadrado, cubo e quarta potência, diferentes entre si).

11. A função de Euler

Se a é um inteiro e $p > 1$ é um número primo que não divide a, então $a^{p-1} - 1$ é um múltiplo de p. Foi isso, no fundo, que Fermat comunicou a seu amigo Frénicle de Bessy, em carta de 18 de outubro de 1640, na qual comentava também ter uma demonstração desse resultado. Mas, se a tinha, não a deixou entre seus escritos e muito menos a publicou. Assim é que somente no século seguinte, em 1736, seria publicada a primeira demonstração desse teorema — hoje chamado pequeno teorema de Fermat. O mérito coube, como em outras vezes, a Euler. Em 1760 Euler conseguiu uma generalização desse teorema para a qual teve de introduzir a função hoje conhecida pelo seu nome e que definiremos a seguir.

DEFINIÇÃO 9 A função $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ que associa a cada $m \in \mathbb{N}^*$ o número de elementos do conjunto $\{k \in \mathbb{N}^* \mid 1 \leqslant k \leqslant m$ e $\text{mdc}(k, m) = 1\}$ é chamada *função φ de Euler*.

Ou seja $\varphi(m)$ indica quantos dos números da seqüência

$$1, 2, \ldots, m-1, m \text{ (ou } 0, 1, 2, \ldots, m-1 \text{, o que é equivalente)}$$

são primos com m. Às vezes φ é conhecida também como *indicador de Euler*.

Por exemplo: $\varphi(8) = 4$ porque, de 1 a 8 (inclusive), os números primos com 8 são aqueles destacados a seguir:

$$\mathit{1}, 2, \mathit{3}, 4, \mathit{5}, 6, \mathit{7}, 8$$

Se p é primo, como de 1 a p o único elemento não primo com p é o próprio p, então $\varphi(p) = p - 1$.

Numa situação um pouco mais geral, se p é primo e $m = p^\alpha$ ($\alpha \geqslant 1$), quais dos elementos de

$$1, 2, \ldots, p^\alpha$$

não são primos com $m = p^\alpha$? Somente aqueles que são múltiplos de p, ou seja:

$$p, 2p, \ldots, p^{\alpha-1} \cdot p$$

Como há $p^{\alpha-1}$ elementos nesta última seqüência e p^α na anterior, então:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

TEOREMA 3 (Euler) Para todo inteiro $m > 1$ e para todo $a \in \mathbb{Z}$, primo com m, vale a congruência:

$$a^{\varphi(m)} \equiv 1 \pmod m$$

Demonstração: Sejam $s_1, s_2, \ldots, s_k$ os inteiros de 1 a m, inclusive os extremos, que são primos com m (logo $k = \varphi(m)$). Dividamos cada as_i por m:

$$as_i = mq_i + r_i \; (0 \leqslant r_i < m)$$

Se existisse um primo p tal que $p \mid m$ e $p \mid r_i$, dessa igualdade decorreria que $p \mid as_i$. Mas então $p \mid a$ ou $p \mid s_i$, o que é impossível já que $\text{mdc}(a, m) = 1$ (hipótese) e ainda $\text{mdc}(m, s_i) = 1$, devido à escolha dos s_i. Donde m e r_i são primos entre si, para todo i, $1 \leqslant i \leqslant k$.

Mostremos agora que na seqüência de restos $r_1, r_2, \ldots, r_k$ não há elementos repetidos. De fato, se $r_i = r_j$ ($1 \leqslant i, j \leqslant k$; $i \neq j$), então $as_i - mq_i = as_j - mq_j$ e portanto $a(s_i - s_j) = m(q_i - q_j)$. Como $\text{mdc}(a, m) = 1$, então $m \mid (s_i - s_j)$. Como $1 \leqslant s_i, s_j \leqslant m$, então teríamos que ter $s_i = s_j$, o que não é possível, posto que $i \neq j$.

Disso tudo decorre então que $\{s_1, s_2, \dots, s_k\} = \{r_1, r_2, \dots, r_k\}$. Assim, se multiplicarmos as congruências $as_i \equiv r_i \pmod m$ decorrentes de $as_i = mq_i + r_i$ $(1 \leqslant i \leqslant k)$:

$$a^k s_1 s_2 \dots s_k \equiv (as_1)(as_2) \dots (as_k) \equiv r_1 r_2 \dots r_k \pmod m$$

os produtos $s_1 s_2 \dots s_k$ e $r_1 r_2 \dots r_k$ que nela aparecem são iguais. Como m é primo com cada r_i (ou s_i) e, portanto, com o produto $r_1 r_2 \dots r_k$, então esse produto pode ser cancelado na última congruência, resultando a tese:

$$a^{\varphi(m)} \equiv 1 \pmod m$$

pois $k = \varphi(m)$. ■

COROLÁRIO 1 (pequeno teorema de Fermat): Se $p > 1$ é um número primo que não divide o inteiro a, então:

$$a^{p-1} \equiv 1 \pmod p$$

Basta lembrar que se p é primo, então $\varphi(p) = p - 1$. ■

COROLÁRIO 2 Se p é um número primo positivo, então

$$a^p \equiv a \pmod p$$

para todo $a \in \mathbb{Z}$.

Demonstração: Se $\text{mdc}(a, p) = 1$, então, pelo corolário anterior:

$$a^{p-1} \equiv 1 \pmod p$$

Daí, multiplicando por p:

$$a^p \equiv p \pmod p$$

Se $\text{mdc}(a, p) \neq 1$, então $a \equiv 0 \pmod p$, pois p é primo. Donde:

$$a^p \equiv 0 \equiv a \pmod p$$ ■

Exemplo 17: Se $a > 0$ é um inteiro, mostremos que a e a^5 têm o mesmo algarismo das unidades.

Se a_0 e a'_0, respectivamente, indicam esses algarismos, então

$$a = 10q + a_0$$

e

$$a^5 = 10q' + a'_0$$

Assim:

$$a^5 - a = 10(q' - q) + (a'_0 - a_0)$$

Notemos que se $a_0 = a'_0$, então $10 \mid (a^5 - a)$. Por outro lado, se $10 \mid (a^5 - a)$, então $10 \mid (a'_0 - a_0)$ e portanto $a'_0 = a_0$, já que $0 \leqslant a_0, a'_0 \leqslant 9$. Basta provar então que $a^5 - a$ é múltiplo de 10.

Mas o corolário 2 nos assegura que $a^5 \equiv a \pmod 5$, do que segue: $5 \mid (a^5 - a)$. Por outro lado, como $a \equiv 0, 1 \pmod 2$, então $a^5 \equiv 0, 1 \pmod 2$ e portanto $a^5 - a \equiv 0 \pmod 2$, ou seja, $2 \mid (a^5 - a)$. O fato de 2 e 5 serem primos entre si garante então que $10 \mid (a^5 - a)$.

LEMA Se $\{r_1, r_2, \dots, r_m\}$ é um sistema completo de restos módulo m, então há nesse conjunto exatamente $\varphi(m)$ elementos primos com m.

Demonstração: Como $\{0, 1, \dots, m - 1\}$ é um sistema completo de restos módulo m, então cada r_i é côngruo, módulo m, a um, e apenas um elemento desse conjunto. Digamos:

$$r_i \equiv i - 1 \pmod m \quad (i = 1, 2, \dots, m)$$

ou

$$r_i = (i - 1) + k_i m$$

para convenientes $k_i \in \mathbb{Z}$ $(i = 1, 2, \dots, m)$.
Mas daí segue, devido à proposição 6, que:

$$\text{mdc}(r_i, m) = 1 \iff \text{mdc}(i - 1, m) = 1$$

Portanto, há tantos elementos em $\{r_1, r_2, \dots, r_m\}$ primos com m quantos há em $\{0, 1, \dots, m - 1\}$, primos com m, ou seja, $\varphi(m)$. ■

PROPOSIÇÃO 17 Se m e n são números naturais não nulos primos entre si, então:

$$\varphi(mn) = \varphi(m)\,\varphi(n)$$

Demonstração: Formemos o quadro

1	2	3	$\dots$	$n - 1$	n
$1 + n$	$2 + n$	$3 + n$	$\dots$	$(n - 1) + n$	$2n$
$1 + 2n$	$2 + 2n$	$3 + 2n$	$\dots$	$(n - 1) + 2n$	$3n$
.....	.....	.....	.....	.....	.....
$1 + (m-1)n$	$2 + (m-1)n$	$3 + (m-1)n$	$\dots$	$(n-1) + (m-1)n$	mn

que compreende todos os números naturais de 1 a mn, inclusive os $\varphi(mn)$ elementos primos com mn, que nos interessam. Estes, nós os encontraremos cancelando no quadro todos os números que não são primos com mn, entre os quais estão aqueles que não são primos com n.

Ora, se s está na primeira linha e não é primo com n, o mesmo acontece com todos os elementos $s + kn$ da coluna de s. De fato, se $d \mid n$ e $d \mid s$, então decorre de $\mathbf{d_4}$, item 6.1, que $d \mid (s + kn)$. Então, todas as colunas nessas con-

dições podem ser canceladas totalmente. Restarão as colunas encabeçadas por elementos que são primos com n, ou seja, $\varphi(n)$ colunas.

Observemos, por outro lado, que em cada coluna dois elementos quaisquer, não da mesma linha, são incôngruos, módulo m. De fato, se

$$k + in \equiv k + jn \pmod m$$

onde, por exemplo, $i > j$, então

$$(i - j)n \equiv 0 \pmod m$$

e daí $m \mid (i - j)n$; como $mdc(m, n) = 1$, então $m \mid (i - j)$; mas isso é absurdo pois $0 \leqslant j < i < m$, e portanto $i - j < m$.

Logo, cada coluna é um sistema completo de restos, módulo m, e assim, em cada coluna não cancelada, riscando os elementos não primos com m, restam (em virtude do lema) $\varphi(m)$ elementos. Como são $\varphi(n)$ estas colunas, restam sem cancelar $\varphi(n)\varphi(m)$ elementos do quadro.

Mas conforme exercício resolvido número 220:

$$mdc(a, mn) \neq 1 \iff mdc(a, m) \neq 1 \text{ ou } mdc(a, n) \neq 1$$

Isso em particular significa que cancelar no quadro construído os elementos que não são primos com n, mais os que não são primos com m, equivale a cancelar os que não são primos com mn. Assim, podemos dizer também que deixamos de cancelar $\varphi(mn)$ elementos, e portanto:

$$\varphi(m)\varphi(n) = \varphi(mn)$$ ■

Nota: Uma função $f: \mathbb{N}^* \to \mathbb{N}^*$ para a qual $f(mn) = f(m)f(n)$, sempre que $mdc(m, n) = 1$, chama-se *função multiplicativa*. Logo φ é multiplicativa.

Exemplo 18: Vamos supor m = 4 e n = 5:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

Na primeira linha o único elemento não primo com n = 5 é o próprio 5, daí termos eliminado a coluna do 5. Em cada uma das outras colunas há dois elementos não primos com 4: 6 e 16 na primeira, 2 e 12 na segunda, 8 e 18 na terceira e 4 e 14 na quarta. Os elementos restantes:

1, 3, 7, 9, 11, 13, 17, 19

são os inteiros de 1 a 20 primos com 20. Portanto $\varphi(20) = 8$.

COROLÁRIO Sejam $m_1, m_2, \ldots, m_r \in \mathbb{N}^*$ tais que $mdc(m_i, m_j) = 1$, sempre que $i \neq j$. Então

$$\varphi(m_1 m_2 \ldots m_r) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_r)$$

Para r = 1 o resultado é imediato. Vamos supô-lo válido para $r - 1 \geqslant 1$. Como

$$\varphi(m_1 m_2 \ldots m_r) = \varphi(m_1 m_2 \ldots m_{r-1})\,\varphi(m_r)$$

pois $mdc(m_1 m_2 \ldots m_{r-1}, m_r) = 1$, e como

$$\varphi(m_1 m_2 \ldots m_{r-1}) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_{r-1})$$

pela hipótese de indução, o resultado vale também para r. ■

TEOREMA 4 Se $m > 1$ é um inteiro cujos fatores primos são $p_1, p_2, \ldots p_r$, onde $p_i \neq p_j$, sempre que $i \neq j$, então:

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

Demonstração: Por hipótese

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r} \qquad (\alpha_i \geqslant 1)$$

onde, é claro,

$$mdc\,(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \qquad (\text{para } i \neq j)$$

Levando em conta que

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

como já foi demonstrado, a proposição anterior e seu corolário nos asseguram que:

$$\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_r^{\alpha_r}) =$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\ldots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

$$= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$ ■

Por exemplo: Se $m = 60 = 2^2 \cdot 3 \cdot 5$, então

$$\varphi(m) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$$

EXERCÍCIOS

303. Calcule: $\varphi(200)$, $\varphi(860)$ e $\varphi(1\ 001)$.

304. Se n = 5 186, verifique as seguintes igualdades: $\varphi(n) = \varphi(n+1) = \varphi(n+2)$.

305. Considere os números $m = 3^r \cdot 144$ e $n = 3^r \cdot 95$, onde $r \geq 0$. Mostre que $\varphi(m) = \varphi(n)$.

306. Mostre que: $\varphi(n) = n - 1 \iff n$ é primo.

Resolução: $\Rightarrow$ Vamos supor n não primo. Então n admite um divisor r, $1 < r < n$, e portanto $mdc(n, r) = r > 1$. Assim, há pelo menos dois elementos em $\{1, 2, \ldots, n\}$ não primos com n: r e n. Mas isto implica que $\varphi(n)$ é no máximo igual a $n - 2$. Absurdo.

307. Mostre que se $d|n$, então $\varphi(d)|\varphi(n)$.

308. Mostre que $\varphi(m^2) = m\varphi(m)$, para todo $m \geq 1$.

309. Prove as seguintes afirmações:

a) Se n é ímpar, então $\varphi(2n) = \varphi(n)$

b) Se n é par, então $\varphi(2n) = 2\varphi(n)$

c) $\varphi(3n) = 3\varphi(n) \iff 3|n$

d) $\varphi(3n) = 2\varphi(n) \iff 3\nmid n$

Resolução de b): Se n é par e $n = 2^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ é sua decomposição canônica, então a de 2n é $2n = 2^{\alpha_1+1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ e portanto:

$$\varphi(2n) = 2n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right) = 2\varphi(n)$$

Resolução de d):

($\Rightarrow$) Vamos supor que $3|n$. Então, devido a c), $\varphi(3n) = 3\varphi(n)$, o que contraria a hipótese.

($\Leftarrow$) Se $3\nmid n$, então na decomposição canônica de n não aparece o fator 3. Digamos, $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ ($p_i \neq 3$, $i = 1, 2, \ldots, r$). Logo $3n = 3 \cdot p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ é a decomposição de 3n em fatores primos e

$$\varphi(3n) = 3n\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_r}\right) = 2\varphi(n)$$

310. Se p e $2p - 1$ são números primos ímpares e $n = 2(2p - 1)$, mostre que $\varphi(n) = \varphi(n + 2)$.

311. Se p e $2p + 1$ são primos ímpares e $n = 4p$, mostre que $\varphi(n + 2) = \varphi(n) + 2$.

312. Seja n um inteiro positivo em cuja decomposição canônica figuram r fatores primos ímpares distintos. Prove que $2^r|\varphi(n)$.

313. Seja n um número natural par tal que $\varphi(n) = \frac{n}{2}$. Prove que $n = 2^r$, para algum $r \geq 1$.

Resolução: Podemos escrever $n = 2^r \cdot q$, onde $r \geq 1$ e q é o produto dos fatores primos de n, distintos de 2. Então $mdc(2^r, q) = 1$ e portanto $\varphi(n) = \varphi(2^r)\varphi(q) = 2^{r-1}\varphi(q)$. Mas por hipótese $\varphi(n) = \frac{n}{2} = 2^{r-1} \cdot q$. Logo $2^{r-1}\varphi(q) = 2^{r-1} \cdot q$, o que implica $\varphi(q) = q$. Mas isso só é possível para $q = 1$ (justifique). Logo $n = 2^r$.

314. Seja $d = mdc(m, n)$. Mostre que:

$\varphi(mn)\varphi(d) = d\varphi(m)\varphi(n)$

315. a) Seja $m > 1$ e considere a congruência $ax \equiv b \pmod m$, onde $mdc(a, m) = 1$. Mostre que $x_0 = a^{\varphi(m)-1} \cdot b$ é uma solução particular dessa congruência linear.

b) Use a parte a) para achar soluções particulares de $5x \equiv 21 \pmod{14}$ e $21x \equiv 30 \pmod{25}$.

316. Sejam a e n inteiros maiores que 1 e tais que $mdc(a, n) = mdc(a - 1, n) = 1$. Prove que: $1 + a + a^2 + \ldots + a^{\varphi(n)-1} \equiv 0 \pmod n$

Sugestão: Fatore $a^{\varphi(n)} - 1$

317. Seja $p > 2$ um número primo. Prove que:

$1^{p-1} + 2^{p-1} + \ldots + (p - 1)^{p-1} \equiv -1 \pmod p$.

Sugestão: Use o pequeno teorema de Fermat para cada uma das parcelas do primeiro membro.

318. Calcule, usando o teorema de Euler:

a) $3^{1000} \equiv ? \pmod 7$

b) $7^{1000} \equiv ? \pmod{54}$

c) $7^{1015} \equiv ? \pmod{31}$

Resolução de b): Como $\varphi(54) = 18$ e mdc(7, 54) = 1, então $7^{18} \equiv 1 \pmod{54}$. Observando que $1\,000 = 18 \cdot 55 + 10$, então $7^{1000} \equiv 7^{10} \pmod{54}$. Mas $7^2 = 49 \equiv -5 \pmod{54}$, $7^4 \equiv 25 \pmod{54}$, $7^8 \equiv 625 \equiv 31 \pmod{54}$ e portanto $7^{10} \equiv -155 \equiv 7 \pmod{54}$. Donde $7^{1000} \equiv 7 \pmod{54}$.

319. Mostre que a^{n+4} e a^n têm o mesmo algarismo das unidades, para quaisquer inteiros a e n, ambos maiores que zero.

320. Seja $a > 0$ um inteiro tal que mdc(a, 5) = 1. Mostre que, para todo inteiro $n > 0$, vale:

$$a^{8n} + 3a^{4n} + 1 \equiv 0 \pmod 5$$

Sugestão: Pequeno teorema de Fermat.

321. Seja $u : \mathbb{N}^* \to \mathbb{Z}$ a função definida por:

a) $u(1) = 1$

b) $u(n) = 0$ se $p^2 | n$, para algum primo p

c) $u(n) = (-1)^r$ se $n = p_1 p_2 \dots p_r$ é um produto de fatores primos distintos entre si.

Esta função, importante em teoria dos números, é chamada *função de Möbius*, em homenagem ao matemático alemão A.F. Möbius (1790-1868), aluno de Gauss, que a introduziu com vistas ao seguinte problema:

"Se duas funções aritméticas (ou seja, duas funções definidas em $\mathbb{N}^*$) f e g estão relacionadas por

$$f(n) = \sum_{d|n} g(d)$$

é possível expressar g em termos de f?"

Isto posto:

i Calcule $\mu(n)$ nos seguintes casos: n = 4, n = 12, n = 86, n = 105 e n = 120.

ii Prove que μ é multiplicativa, isto é, $\mu(mn) = \mu(m)\,\mu(n)$, sempre que mdc(m, n) = 1.

Resolução: Se existe um primo p tal que $p^2 | m$ ou $p^2 | n$, então $p^2 | mn$ e daí

$$\mu(mn) = 0 = \mu(m)\,\mu(n)$$

Caso contrário, $m = p_1 p_2 \dots p_r$ e $n = q_1 q_2 \dots q_s$ onde os p_i e os q_j são primos distintos entre si (lembrar que mdc(m, n) = 1). Então:

$$\mu(mn) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m)\,\mu(n)$$

iii Prove que $\sum_{d|n} \mu(d) = 1$ se $n = 1$ e $\sum_{d|n} \mu(d) = 0$ se $n > 1$.

Sugestão: Se $n > 1$, considere os casos $n = p^a$ e $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_r^{a_r}$ (decomposição canônica de n; $r > 1$) e, para este último, aplique a multiplicatividade de μ.

iv Se $f(n) = \sum_{d|n} g(d)$, prove que $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$ (*fórmula de inversão de Möbius*)

Resolução:

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} g(c) = \sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) g(c)\right)$$

Mas: $d|n$ e $c|\frac{n}{d} \iff c|n$ e $d|\frac{n}{c}$. Mostremos que vale $\Rightarrow$. De fato, como $c|\frac{n}{d}$, então $c|n$, pois n é múltiplo de $\frac{n}{d}$; mas $c|\frac{n}{d}$ se traduz por $\frac{n}{d} = cq$ ($q \in \mathbb{Z}$) e como $c|n$ (acabamos de provar), então $\frac{n}{c} = dq$, ou seja, $d|\frac{n}{c}$. A demonstração de $\Leftarrow$ é análoga.

Assim:

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{c|n} \left(\sum_{d|\frac{n}{c}} g(c)\mu(d)\right) =$$

$$= \sum_{c|n} \left(g(c) \sum_{d|\frac{n}{c}} \mu(d)\right) \overset{(*)}{=} \sum_{c=n} g(c) \cdot 1 = g(n)$$

onde, na passagem (*), usamos **iii**.

v Para todo $n \geqslant 1$, prove que:

$$\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3) = 0$$

Resolução: Vamos supor $n = 2q$ (par). Se o próprio q é par, então $2^2 | n$ e $\mu(n) = 0$. Se q é ímpar, então $n + 2 = 2q + 2 = 2(q + 1)$, onde $q + 1$

é par e portanto $\mu(n + 2) = 0$, pois $2^2|(n + 2)$. O caso n ímpar deixamos como exercício.

vi Se $n \geqslant 3$, prove que:

$$\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \ldots + \mu(n!) = 1$$

vii Vamos supor que a decomposição canônica de um inteiro $a > 1$ seja $a = p_1p_2 \ldots p_r$, onde r é par e $p_i \neq p_j$ sempre que $i \neq j$. Se d percorre o conjunto dos divisores de a tais que $0 < d < \sqrt{a}$, mostre que:

$$\sum_{d} \mu(d) = 0$$

Resolução: Se d é um desses divisores, então d é um produto de alguns fatores de a. Se, por exemplo, $d = p_1p_2 < \sqrt{a}$, então

$$a = p_1p_2p_3 \ldots p_r < \sqrt{a}\, p_3 \ldots p_r$$

e daí

$$\sqrt{a} = \frac{a}{\sqrt{a}} < p_3 \ldots p_r = c$$

E como $\mu(a) = (-1)^r = 1 = (-1)^2(-1)^{r-2} = \mu(d)\,\mu(c)$, então $\mu(d) = \mu(c)$ (= 1, neste caso). De um modo geral, a cada d conforme o enunciado corresponde um divisor c de a tal que $cd = a$ e $c > \sqrt{a}$. Ademais $\mu(d) = \mu(c)$. Levando em conta a parte **iii**:

$$2 \sum_{d} \mu(d) = \sum_{d} \mu(d) + \sum_{c} \mu(c) = \sum_{n|a} \mu(n) = 0$$

12. Restos quadráticos — teorema de Wilson

Seja p um número primo positivo e consideremos um inteiro a não divisível por p. Diz-se que a é um *resto quadrático* de p se existe $b \in \mathbb{Z}_p = \{0, 1, 2, \ldots, p - 1\}$ de maneira que $b^2 \equiv a \pmod p$.

Por exemplo, 4 é um resto quadrático de 5, pois $3^2 \equiv 4 \pmod 5$.

Como $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$ e $4^2 \equiv 1 \pmod 5$, então 2 e 3, por exemplo, não são restos quadráticos de 5.

Usa-se a notação aRp para indicar que a é resto quadrático de p, e aNp se a não é resto quadrático de p.

Vamos supor aRp. Logo, existe $b \in \mathbb{Z}_p$ para o qual $b^2 \equiv a \pmod p$. Então $(p - b)^2 = p^2 - 2bp + b^2 \equiv b^2 \pmod p$, e daí $(p - b)^2 \equiv a \pmod p$. Ademais, se para algum $c \in \mathbb{Z}_p$ se verificar $c^2 \equiv a \pmod p$, então $c^2 \equiv b^2 \pmod p$ e daí $c^2 - b^2 = (c - b)(c + b) \equiv 0 \pmod p$, o que implica $p|(c - b)$ ou $p|(c + b)$. Como $b, c \in \mathbb{Z}_p$, então

$$c - b = 0 \quad \text{ou} \quad c + b = p$$

Ou seja: $c = b$ ou $c = p - b$.

Mantendo ainda a hipótese aRp e admitindo que $b^2 \equiv a \pmod p$, $b \in \mathbb{Z}_p$, observemos o fatorial

$$(p - 1)! = 1 \cdot 2 \ldots b \ldots (p - b) \ldots (p - 2)(p - 1)$$

Para cada $a_0 \in \mathbb{Z}$, $1 \leqslant a_0 < p$, $a_0 \neq b$ e $a_0 \neq p - b$, a congruência $a_0x \equiv a \pmod p$ admite uma solução x_0, $1 \leqslant x_0 < p$, pois a_0 e p são primos entre si, e $x_0 \neq a_0$ (se $x_0 = a_0$, então $a_0^2 \equiv a \pmod p$, o que não é possível, pois $a_0 \neq b$ e $a_0 \neq p - b$).

Logo, os fatores de $(p - 1)!$, excluídos b e $p - b$, podem ser agrupados aos pares de modo que cada um dos produtos resultantes seja côngruo a *a*, módulo p. Como esses fatores, excluídos b e $p - b$, são $p - 3$, então:

$$(p - 1)! \equiv a^{\frac{p-3}{2}} \cdot b \cdot (p - b) \pmod p$$

Como $b(p - b) \equiv -a \pmod p$, então:

$$(p - 1)! \equiv -a^{\frac{p-1}{2}} \pmod p$$

Em particular, isso leva ao

TEOREMA 5 (*teorema de Wilson*): Se p é um número primo positivo, então:

$$(p - 1)! \equiv -1 \pmod p$$

Demonstração: O caso $p = 2$ é imediato. Se $p > 2$, observando que $1^2 \equiv 1 \pmod p$, o que significa que 1Rp, então, levando em conta a conclusão anterior:

$$(p - 1)! \equiv -1^{\frac{p-1}{2}} \equiv -1 \pmod p \qquad \blacksquare$$

Por exemplo, se $p = 7$, como $3^2 \equiv 2 \pmod 7$, então 2 é resto quadrático de 7. Também $(7 - 3)^2 = 4^2 \equiv 2 \pmod 7$. Observando os fatores de $(7 - 1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$, diferentes de 3 e 4, vemos que a solução de $2x \equiv 2 \pmod 7$ em $\mathbb{Z}_7$ é 1 e a de $5x \equiv 2 \pmod 7$ é 6. Logo, a maneira de agrupar os fatores de 6!, segundo o teorema, é:

$$6! = (1 \cdot 2) \cdot (3 \cdot 4) \cdot (5 \cdot 6) \equiv 2 \cdot (-2) \cdot 2 \equiv -1 \pmod 7$$

Mostremos agora que se aNp, onde p é um primo ímpar, então:

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod p$$

De fato, neste caso para cada $a_0 \in \mathbf{Z}$, $1 \leqslant a_0 < p$, a congruência $a_0x \equiv a \pmod p$ admite uma solução x_0, $1 \leqslant x_0 < p$, e $x_0 \neq a_0$ pois a não é resto quadrático. Daí que os fatores de $(p-1)!$ podem ser agrupados dois a dois, sem exceção, de maneira que cada um dos produtos resultantes seja côngruo ao elemento a, módulo p. Sendo $p-1$ os fatores:

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod p$$

Por exemplo, se $p = 5$ e $a = 3$, então a maneira de agrupar os fatores de 4! que se utilizou na justificativa anterior é

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = (4 \cdot 2) \cdot (3 \cdot 1) \equiv 3 \cdot 3 \equiv 3^2 \pmod 5$$

pois o número 2 é solução de $4x \equiv 3 \pmod 5$ e o 1 é solução de $3x \equiv 3 \pmod 5$.

PROPOSIÇÃO 18 (*critério de Euler*) Seja p um primo positivo ímpar e seja a um inteiro não divisível por p. Então: a é um resto quadrático de p se, e somente se,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Demonstração

(⇒) Sendo a um resto quadrático de p, então $b^2 \equiv a \pmod p$, para algum $b \in \mathbf{Z}_p$. Como $\mathrm{mdc}(b, p) = 1$, levando em conta o pequeno teorema de Fermat obtemos:

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$$

(⇐) Suponhamos aNp. Então, devido ao fato de que

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod p$$

como já foi mostrado, da hipótese segue que:

$$(p-1)! \equiv 1 \pmod p$$

Mas $(p-1)! \equiv -1 \pmod p$, em virtude do teorema de Wilson. Logo

$$-1 \equiv 1 \pmod p$$

o que não é possível pois, por hipótese, $p > 2$. ■

Exemplo 19:

Se $p = 11$, então $\frac{p-1}{2} = 5$. Assim, como

$$2^5 = 32 \equiv -1 \pmod{11}$$

2N11. Por outro lado, como $3^2 = 9 \equiv -2 \pmod{11}$, então $3^4 \equiv 4 \pmod{11}$ e portanto $3^5 \equiv 12 \equiv 1 \pmod{11}$, o que garante a relação 3R11.

Nota: Se $p > 1$ é um número primo, dizer que a é resto quadrático de p equivale a dizer que a congruência

$$x^2 \equiv a \pmod p \qquad (p \nmid a)$$

admite solução em $\mathbf{Z}_p$.

O resultado central do capítulo dos restos quadráticos é a chamada "Lei da Reciprocidade Quadrática". Exposta em 1785 por Adrian-Marie Legendre (1752-1833), seria demonstrada pela primeira vez por Gauss, em 1796. Uma maneira de formulá-la é a seguinte:

"Sejam p e q primos ímpares positivos, $p \neq q$, e consideremos o par de congruências

$$x^2 \equiv p \pmod q \quad \text{e} \quad x^2 \equiv q \pmod p.$$

Então, ou ambas admitem solução ou nenhuma delas admite solução, salvo no caso em que p e q são da forma $4n + 3$, hipótese em que uma admite solução e a outra não".

Se introduzirmos o *símbolo de Legendre* definido por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ se aRp} \\ -1 \text{ se aNp} \end{cases}$$

então a lei da reciprocidade quadrática se traduz assim:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

onde p e q são primos positivos ímpares e $p \neq q$.

A demonstração dessa lei foge completamente aos objetivos deste texto. O leitor interessado poderá encontrá-la na bibliografia em [1] e [5], por exemplo.

EXERCÍCIOS

322. Ache os restos quadráticos de 7, 13 e 17.

323. Verdadeiro ou falso: 6R19, 9N19, 4R23, 8N23? Justifique.

324. Seja a um resto quadrático do número primo ímpar p. Mostre que:

a) $p \equiv 1 \pmod 4 \Rightarrow (p - a)Rp$.

b) $p \equiv 3 \pmod 4 \Rightarrow (p - a)Np$.

Sugestão: Use o fato de que $p - a \equiv -a \pmod p$ e o critério de Euler.

325. Seja p um primo ímpar e sejam a e b inteiros tais que $p \nmid a$ e $p \nmid b$. Mostre que:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Portanto, em que condições ab é resto quadrático de p?

326. Use o teorema de Wilson para provar que as soluções de

$$x^2 + 1 \equiv 0 \pmod p;\ p = 4m + 1 \text{ (primo)}$$

são $\pm 1 \cdot 2 \dots 2m \pmod p$.

Resolução: Se a e b são soluções dessa congruência, então $a^2 + 1 \equiv b^2 + 1 \pmod p$ e daí $(a - b)(a + b) \equiv 0 \pmod p$. Logo, considerando que p é primo, $b \equiv a \pmod p$ ou $b \equiv -a \pmod p$.

Observemos porém que, como $p = 4m + 1$: $(p - 1)! + 1 =$
$= (p - 1)(p - 2) \dots (p - 2m)(2m)(2m - 1) \dots 2 \cdot 1 + 1$

$$\equiv (2m)^2 (2m - 1)^2 \dots 2^2 \cdot 1^2 + 1 \equiv 0 \pmod p$$

devido ao teorema de Wilson e ao fato de que $p - 1 \equiv -1 \pmod p$, $p - 2 \equiv -2 \pmod p$, ..., $p - 2m \equiv -2m \pmod p$, onde o número de congruências é 2m (par). Logo $(2m)(2m - 1) \dots 2 \cdot 1$ é uma solução de $x^2 + 1 \equiv 0 \pmod p$, o que conclui o exercício, levando em conta a observação inicial.

327. Seja $p > 2$ um número primo. Mostre que a congruência $x^2 + 1 \equiv 0 \pmod p$ admite soluções se, e somente se, $p \equiv 1 \pmod 4$.

Sugestão: A congruência admite soluções se, e somente se, -1 é resto quadrático de p.

328. Agrupe os fatores do produto

$$2 \cdot 3 \cdot 4 \dots 20 \cdot 21$$

em pares $ab \equiv 1 \pmod{23}$. Justifique o procedimento empregado.

329. Use o teorema de Wilson para mostrar que, se $p > 2$ é primo, então:

$$1^2 \cdot 3^2 \cdot 5^2 \dots (p - 2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

Sugestão: Leve em conta que $2 \equiv -(p - 2) \pmod p$, $p - 3 \equiv -3 \pmod p$, $4 \equiv -(p - 4) \pmod p$, $p - 5 \equiv -5 \pmod p$, ...

330. Seja $p > 2$ um número primo. Use o teorema de Wilson para provar que:

$$1^2 \cdot 3^2 \cdot \dots \cdot (p - 2)^2 \equiv 2^2 \cdot 4^2 \cdot \dots \cdot (p - 1)^2 \pmod p$$

331. Prove a recíproca do teorema de Wilson: "Se $(n - 1)! \equiv -1 \pmod n$, então n é primo".

Resolução: Se n não fosse primo, então admitiria um divisor primo p, $1 < p < n$. Como, então, p é um dos fatores de $(n - 1)! = -1 + nq$ e $p \mid n$, então $p \mid 1$, o que é absurdo.

332. Prove que um inteiro $n > 1$ é primo se, e somente se, $(n - 2)! \equiv 1 \pmod n$.

13. Raízes primitivas

Seja a um número inteiro primo com $m (m \in \mathbb{Z}, m > 1)$. Pelo teorema de Euler

$$a^{\varphi(m)} \equiv 1 \pmod m$$

O menor inteiro $h \geqslant 1$ para o qual

$$a^h \equiv 1 \pmod m$$

chama-se *ordem de a, módulo m*. Se h coincide com $\varphi(m)$, então se diz que a é uma *raiz primitiva* de m.

Por exemplo, se $a = 3$ e $m = 10$, caso em que $\varphi(m) = \varphi(10) = 4$, então:

$$3^1 \equiv 3 \pmod{10} \qquad 3^3 \equiv 27 \equiv 7 \pmod{10}$$
$$3^2 \equiv 9 \pmod{10} \qquad 3^4 \equiv 81 \equiv 1 \pmod{10}$$

o que mostra que 3 é raiz primitiva de 10.

PROPOSIÇÃO 19 Se h é a ordem de a, módulo m, então $a, a^2, \dots, a^{h-1}, a^h$ são mutuamente incôngruos, módulo m.

Demonstração: Vamos supor

$$a^s \equiv a^r \pmod m$$

onde $1 \leqslant s < r \leqslant h$. Como $\text{mdc}(a^s, m) = 1$ pois $\text{mdc}(a, m) = 1$, então o corolário 1 da propriedade C_6 das congruências nos permite concluir (cancelando a^s na congruência de que partimos) que:

$$a^{r-s} \equiv 1 \pmod m$$

Mas isso contraria a hipótese de que a ordem de a, módulo m, é h, pois $1 \leqslant r - s < h$. ■

PROPOSIÇÃO 20 Seja h a ordem de a, módulo m, e consideremos um inteiro $d \geqslant 0$. Então:

$$a^d \equiv 1 \pmod m \iff h \mid d$$

Demonstração

$(\Leftarrow)$ Por hipótese $d = hq$, para algum $q \in \mathbb{Z}$. Como $a^h \equiv 1 \pmod m$, então

$$a^d = (a^h)^q \equiv 1^q \equiv 1 \pmod m$$

$(\Rightarrow)$ Pelo algoritmo da divisão: $d = hq + r$ $(0 \leqslant r < h)$. Daí

$$a^d = a^{hq+r} = (a^h)^q \cdot a^r \equiv a^r \pmod m$$

Como $a^d \equiv 1 \pmod m$, por hipótese, então:

$$a^r \equiv 1 \pmod m$$

Então não se pode ter $0 < r < h$, visto que h é a ordem de a módulo m. Donde $r = 0$ e portanto $d = hq$, ou seja, $h \mid d$. ■

COROLÁRIO Se h é a ordem de a, módulo m, então $h \mid \varphi(m)$.

É só lembrar que, pelo teorema de Euler, $a^{\varphi(m)} \equiv 1 \pmod m$, sempre que $\text{mdc}(a, m) = 1$.

Exemplo 20: Seja $m > 1$ e consideremos um inteiro a primo com m. Então a congruência $ax \equiv 1 \pmod m$ admite soluções em $\mathbb{Z}$. Se b é uma solução qualquer dessa congruência, mostremos que a e b têm a mesma ordem, módulo m. Sejam h e k, respectivamente, essas ordens. Como $a^h \equiv 1 \pmod m$, então $a^h b^h = (ab)^h \equiv b^h \pmod m$. Mas o fato de $ab \equiv 1 \pmod m$ implica $(ab)^h \equiv 1^h \equiv 1 \pmod m$. Donde $b^h \equiv 1 \pmod m$. Como a ordem de b, módulo p, é k, a proposição anterior nos garante que $k \mid h$. De maneira análoga se mostra que $h \mid k$. Donde $h = k$.

EXERCÍCIOS

333. Ache a ordem dos inteiros 4, 7 e 11:

a) módulo 17 b) módulo 25 c) módulo 15

334. Seja p um primo. Se a é um inteiro tal que $p \nmid a$, prove que: a ordem de a, módulo p, é 2 se, e somente se, $a \equiv -1 \pmod p$.

335. Prove cada uma das seguintes afirmações:

a) Se a tem ordem hk, módulo n, então a^h tem ordem k, mod n.
b) Se a ordem do inteiro a, módulo $p > 2$ (p primo) é 2k, então $a^k \equiv -1 \pmod p$.
c) Se a tem ordem $n - 1$, módulo n, então n é primo.

Sugestão para c): Use exercício 306.

336. a) Mostre que o inteiro 2 tem ordem n, mod. $2^n - 1$.
b) Prove que $\varphi(2^n - 1)$ é múltiplo de n, para todo $n > 1$.
c) Se $p > 1$ é primo, pode-se concluir que $\varphi(p^n - 1)$ é múltiplo de n, para todo $n > 1$? Justifique a resposta.

Sugestão para a): $h < n \Rightarrow 2^h - 1 < 2^n - 1$.

337. Vamos supor que a ordem de a módulo n é h e que a ordem de b módulo n é k. Prove que:

a) a ordem de ab módulo n divide hk.
b) Se $\text{mdc}(h, k) = 1$, então a ordem de ab é exatamente hk.

Resolução:

a) Como $(ab)^{hk} = (a^h)^k (b^k)^h \equiv 1 \pmod n$, a proposição 20 garante que hk é múltiplo da ordem de ab, módulo n.
b) Seja d a ordem de ab, módulo n. Então $(ab)^d \equiv 1 \pmod n$ e portanto $(ab)^{dh} = (a^h)^d \cdot b^{dh} \equiv 1 \pmod n$; como porém $(a^h)^d \equiv 1 \pmod n$, pois a tem ordem h, módulo n, então $b^{dh} \equiv 1 \pmod n$, o que implica $k \mid (dh)$; como porém $\text{mdc}(h, k) = 1$, então $k \mid d$. Analogamente se mostra que $h \mid d$. Donde $(hk) \mid d$, pois $\text{mdc}(h, k) = 1$. Mas em a) já havíamos obtido que $d \mid (hk)$. Donde $d = hk$.

338. Seja $a > 1$ um inteiro. Se $p > 2$ é primo, prove que os divisores ímpares primos de $a^p - 1$ ou são também divisores de $a - 1$ ou são da forma $2px + 1$.

339. Seja $a > 1$ um inteiro. Se $p > 2$ é primo, prove que os divisores primos ímpares de $a^p + 1$ ou dividem $a + 1$ ou são da forma $2px + 1$.

Resolução: Se q é um primo ímpar, divisor de $a^p + 1$, então $a^p + 1 \equiv 0 \pmod q$ e daí $a^{2p} \equiv 1 \pmod q$. Logo, as possíveis ordens de a, módulo q, são $d = 1, 2$, p ou 2p.

Vamos supor $d = 1$. Então $a \equiv 1 \pmod q$ e daí $a^p \equiv 1 \pmod q$; mas como $a^p \equiv -1 \pmod q$, então $1 \equiv -1 \pmod q$, o que não é possível pois q é ímpar. Se $d = p$, então igualmente teríamos $a^p \equiv 1 \pmod q$, o que contradiz $a^p \equiv -1 \pmod q$. No caso $d = 2$ se tem $a^2 \equiv 1 \pmod q$; daí $q \mid (a-1)(a+1)$, o que implica $q \mid (a-1)$ ou $q \mid (a+1)$, ou seja, $a \equiv 1 \pmod q$ ou $a \equiv -1 \pmod q$.
Como a primeira possibilidade corresponde a $d = 1$ deve ser descartada, restando $a \equiv -1 \pmod q$, o que equivale a $q \mid (a+1)$.
Finalmente, se $d = 2p$, como $\varphi(q) = q - 1$ é múltiplo de $2p$, então $q = 1 + 2px$.

340. Mostre que há infinitos números primos da forma $2px + 1$, onde $p > 2$ é primo.

Sugestão: Todo divisor primo de $2^p - 1$ é da forma $2px + 1$ (exerc. 338). Suponha que $p_1, p_2, \ldots, p_r$ fossem todos os primos da forma dada. Considere o número $(p_1 \cdot p_2 \ldots p_r)^p - 1$ e use o exercício 338.

341. Prove as seguintes afirmações:

a) Os divisores primos ímpares de um inteiro $n^2 + 1$ são da forma $4k + 1$.

b) Os divisores primos ímpares de um número inteiro $n^4 + 1$ são da forma $8k + 1$.

342. Prove que há infinitos números primos da forma $4k + 1$.

343. Prove que há infinitos números primos da forma $8k + 1$.

344. Seja p um primo ímpar. Se $p \nmid a$, mostre que $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$.

345. a) Mostre que 2 é raiz primitiva de 19, mas não é de 17.

b) Mostre que 15 não admite raízes primitivas.

346. Seja a um resto quadrático de um primo ímpar p. Mostre que a não é raiz primitiva de p.

347. Seja a uma raiz primitiva de um primo ímpar p. Prove que:

a) Se $p \equiv 1 \pmod 4$, então $-a$ também é raiz primitiva de p.

b) Se $p \equiv 3 \pmod 4$, então a ordem de $-a$, módulo p, é $\dfrac{p-1}{2}$.

348. Sejam a e b raízes primitivas de um primo ímpar p. Prove que ab não é raiz primitiva de p.

Resolução: Como a é raiz primitiva de p, então $\varphi(p) = p - 1$ é o menor expoente estritamente positivo para o qual $a^{p-1} - 1 \equiv 0 \pmod p$. Daí $\left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p$ e portanto $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, posto que a ordem de a é $p - 1$. Analogamente, $b^{\frac{p-1}{2}} \equiv -1 \pmod p$. Donde $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod p$ e a ordem de ab, módulo p, é menor que $\varphi(p)$.

349. Se $p = 2^k + 1$ é primo e se a não é resto quadrático de p, prove que a é raiz primitiva, módulo p.

350. Seja a uma raiz primitiva de n. Se $k > 0$ e se $\text{mdc}(k, \varphi(n)) = 1$, prove que a^k também é raiz primitiva de n.

351. Seja $n > 1$ um inteiro.

a) Se a é raiz primitiva de n, mostre que os elementos de $A = \{a, a^2, \ldots, a^{\varphi(n)}\}$ são mutuamente incôngruos, módulo n.

b) Se $a_1, a_2, \ldots, a_{\varphi(n)}$ indicam os inteiros positivos menores que n e primos com n, prove que todo elemento de A é côngruo, módulo n, a um único elemento a_i.

Resolução de b): Dividamos a^i $(1 \leqslant i \leqslant \varphi(n))$ por n: $a^i = n \cdot q_i + r_i$ $(0 \leqslant r_i < n)$. Como $\text{mdc}(a, n) = 1$, então $\text{mdc}(a^i, n) = 1$ e portanto $\text{mdc}(n, r_i) = 1$. Logo r_i é um dos elementos de $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$. Como $a^i \equiv r_i \pmod n$, então cada a^i é côngruo, módulo n, a algum dos a_j $(1 \leqslant j \leqslant \varphi(n))$. Não podemos ter $a^i \equiv a_r \pmod n$ e $a^i \equiv a_s \pmod n$, $1 \leqslant r, s \leqslant \varphi(n)$, pois isto obriga $a_r \equiv a_s \pmod n$, o que não é possível, já que $0 \leqslant a_r, a_s < n$.

APÊNDICE II

CONSTRUÇÃO LÓGICO-FORMAL DO CONJUNTO DOS NÚMEROS INTEIROS

1. Os números inteiros: construção

Nosso objetivo aqui é dar um sentido matemático a todas as expressões do tipo a − b, para quaisquer a, b ∈ IN, de maneira a poder tratar como entes do mesmo conjunto tanto aquelas como 7 − 3, 5 − 1 e 4 − 0 quanto aquelas como 3 − 7, 1 − 3 e 0 − 2, por exemplo. Nesse sentido convém observar primeiro que subjacente a cada "diferença" a − b está o par ordenado (a, b) ∈ IN × IN. Além disso é fácil ver que, por exemplo, a igualdade em IN

$$5 - 3 = 9 - 7$$

equivale a 5 + 7 = 9 + 3. De uma maneira geral, se a, b, c, d ∈ IN, a ⩾ b e c ⩾ d, vale a equivalência:

$$a - b = c - d \iff a + d = c + d$$

Essas considerações, aliadas ao fato de que o conjunto dos inteiros a ser construído, deve ser uma "ampliação" de IN, ajudam a entender o caminho que tomaremos.

No conjunto IN × IN consideremos a relação ∼ definida da seguinte maneira: para quaisquer (a, b) e (c, d) em IN × IN,

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Para a relação ∼ valem as propriedades:

- *Reflexiva* pois, como para todo (a, b) ∈ IN × IN, se verifica a + b = b + a, então (a, b) ∼ (a, b).
- *Simétrica*, ou seja, se (a, b) ∼ (c, d), então (c, d) ∼ (a, b) (exercício)
- *Transitiva* pois, se (a, b) ∼ (c, d) e (c, d) ∼ (e, f), então a + d = b + c e c + f = e + d; daí a + d + f = b + c + f e c + f + b = e + d + b, o que

implica a + d + f = e + d + b e portanto a + f = e + b, ou seja: (a, b) ∼ (e, f).

Logo ∼ é uma relação de equivalência em IN × IN e, por conseguinte, determina uma partição neste conjunto em classes de equivalência. Para cada (a, b) ∈ IN × IN, indicaremos por $\overline{(a, b)}$ a classe de equivalência determinada por (a, b) ∈ IN × IN. Assim:

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid (x, y) \sim (a, b)\} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x + b = y + a\}$$

O conjunto quociente de IN × IN por ∼, ou seja, o conjunto de todas as classes $\overline{(a, b)}$, para qualquer (a, b) ∈ IN × IN, será indicado por **Z**. Então:

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim = \{\overline{(a, b)} \mid (a, b) \in \mathbb{N} \times \mathbb{N}\}$$

Por exemplo:

$$\overline{(4, 2)} = \{(2, 0); (3, 1); (4, 2); \ldots\}$$
$$\overline{(2, 4)} = \{(0, 2); (1, 3); (2, 4); \ldots\}$$
$$\overline{(1, 5)} = \{(0, 4); (1, 5); (2, 6); \ldots\}$$

É claro que: $\overline{(a, b)} = \overline{(c, d)} \iff (a, b) \sim (c, d) \iff a + d = b + c$. Em particular vale o seguinte: se a ⩾ b, então $\overline{(a, b)} = \overline{(a - b, 0)}$, pois a + 0 = (a − b) + b; e se b ⩾ a, então $\overline{(a, b)} = \overline{(0, b - a)}$, uma vez que a + (b − a) = b + 0. Assim, se $\overline{(a, b)} \in \mathbb{Z}$, então $\overline{(a, b)} = \overline{(c, 0)}$ ou $\overline{(a, b)} = \overline{(0, c)}$, para algum c ∈ IN. E essa maneira de representar o elemento $\overline{(a, b)}$ é única pois, por exemplo, se $\overline{(c, 0)} = \overline{(d, 0)}$, então c + 0 = d + 0 e daí c = d.

1.1 Adição em Z

Consideremos os números naturais 4 e 3 escritos sob a forma: 4 = 5 − 1 e 3 = 7 − 4. Então: 4 + 3 = (5 − 1) + (7 − 4) = (5 + 7) − (1 + 4). Essa observação ajuda a entender a definição a seguir:

DEFINIÇÃO 1 Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ elementos quaisquer de **Z**. Chama-se *soma de* m *com* n, e se indica por m + n, o elemento de **Z** definido por:

$$m + n = \overline{(a + c, b + d)}$$

Suponhamos $m = \overline{(a, b)} = \overline{(a_1, b_1)}$ e $n = \overline{(c, d)} = \overline{(c_1, d_1)}$; então $m + n = \overline{(a + c, b + d)}$ e $m + n = \overline{(a_1 + c_1, b_1 + d_1)}$. Como porém $(a, b) \sim (a_1, b_1)$ e $(c, d) \sim (c_1, d_1)$, então $a + b_1 = b + a_1$ e $c + d_1 = d + c_1$, do que resulta (somando membro a membro essas igualdades): $(a+b_1) + (c + d_1) = (b + a_1) + (d + c_1)$ ou $(a + c) + (b_1 + d_1) = (b + d) + (a_1 + c_1)$.

Donde $\overline{(a + c, b + d)} = \overline{(a_1 + c_1, b_1 + d_1)}$. Logo a relação dada por

$$(m, n) \rightarrow m + n$$

é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ e portanto é uma operação sobre $\mathbb{Z}$. A essa operação chama-se *adição* em $\mathbb{Z}$.

Para a adição em $\mathbb{Z}$ valem as seguintes propriedades:

a_1 *Associativa*

De fato, se $m = \overline{(a, b)}$, $n = \overline{(c, d)}$ e $r = \overline{(e, f)}$ são elementos genéricos de $\mathbb{Z}$, então:

$$(m + n) + r = \overline{(a + c, b + d)} + \overline{(e, f)} = \overline{((a + c) + e, (b + d) + f)} =$$
$$= \overline{(a + (c + e), b + (d + f))} = \overline{(a, b)} + \overline{(c + e, d + f)} =$$
$$= \overline{(a, b)} + (\overline{(c, d)} + \overline{(e, f)}) = m + (n + r)$$

a_2 *Comutativa*: $m + n = n + m$, $\forall m, n \in \mathbb{Z}$. Exercício.

a_3 Existe *elemento neutro*: é a classe $\overline{(0, 0)}$. De fato, para qualquer $\overline{(a, b)} \in \mathbb{Z}$:

$$\overline{(a, b)} + \overline{(0, 0)} = \overline{(a + 0, b + 0)} = \overline{(a, b)}$$

É óbvio que $\overline{(a, a)} = \overline{(0, 0)}$, para todo $a \in \mathbb{N}$. Usaremos a notação: $0 = \overline{(0, 0)}$, a qual será justificada no item 2.

a_4 Todo $m = \overline{(a, b)} \in \mathbb{Z}$ admite *oposto* (simétrico aditivo). Ou seja, para todo $m \in \mathbb{Z}$ existe $m' \in \mathbb{Z}$ de modo que $m + m' = 0$. Usaremos a notação: $-m = m'$.

Como

$$\overline{(a, b)} + \overline{(b, a)} = \overline{(a + b, b + a)} = 0$$
$$\text{então: } m = \overline{(a, b)} \Rightarrow -m = \overline{(b, a)}.$$

Destaquemos ainda a *lei do cancelamento* em $\mathbb{Z}$:

$$m + r = n + r \Rightarrow m = n$$

De fato: $m = m + 0 = m + [r + (-r)] = (m + r) + (-r) =$
$= (n + r) + (-r) = n + [r + (-r)] = n + 0 = n.$

1.2 Subtração em $\mathbb{Z}$

Para cada par de elementos $m, n \in \mathbb{Z}$, chama-se diferença entre m e n e indica-se por $m - n$ o elemento $m + (-n) \in \mathbb{Z}$. Ou seja:

$$m - n = m + (-n)$$

Assim, posto que $m - n \in \mathbb{Z}$, quaisquer que sejam $m, n \in \mathbb{Z}$, a relação dada por

$$(m, n) \rightarrow m - n$$

é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ — ou seja, é uma operação sobre $\mathbb{Z}$. A essa operação denominamos *subtração* em $\mathbb{Z}$. Esta operação, contudo, não é associativa, nem comutativa e tampouco admite elemento neutro. Sugerimos ao leitor verificar esses fatos.

1.3 Multiplicação em $\mathbb{Z}$

Uma maneira pouco prática de multiplicar os números naturais $3 = 5 - 2$ e $4 = 10 - 6$ seria a seguinte:

$$3 \cdot 4 = (5 - 2) \cdot (10 - 6) = (5 \cdot 10 + 2 \cdot 6) - (5 \cdot 6 + 2 \cdot 10) = 62 - 50 = 12$$

Contudo, a partir daí fica mais fácil entender a

DEFINIÇÃO 2 Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ elementos genéricos de Z. Chama-se *produto* de m por n e indica-se por mn (ou $m \cdot n$) o elemento de $\mathbb{Z}$ definido por:

$$mn = \overline{(ac + bd, ad + bc)}$$

Se $m = \overline{(a, b)} = \overline{(a_1, b_1)}$ e $n = \overline{(c, d)} = \overline{(c_1, d_1)}$, então $mn = \overline{(ac + bd, ad + bc)}$ e $mn = \overline{(a_1c_1 + b_1d_1, a_1d_1 + b_1c_1)}$. Mas como $(a, b) \sim (a_1, b_1)$ e $(c, d) \sim (c_1, d_1)$, então $a + b_1 = b + a_1$ e $c + d_1 = d + c_1$. Daí obtemos: $c(a + b_1) = c(b + a_1)$, $a_1(c + d_1) = a_1(d + c_1)$, $d(b + a_1) = d(a + b_1)$ e $b_1(d + c_1) = b_1(c + d_1)$. Desenvolvendo esses produtos e depois somando membro a membro as igualdades obtidas, feitos a seguir os cancelamentos possíveis, restará

$$(ac + bd) + (a_1d_1 + b_1c_1) = (bc + ad) + (a_1c_1 + b_1d_1)$$

o que pode ser traduzido por:

$$\overline{(ac + bd, ad + bc)} = \overline{(a_1c_1 + b_1d_1, a_1d_1 + b_1c_1)}$$

Isso significa que a relação

$$(m, n) \rightarrow mn$$

é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ e, por isso, uma operação sobre $\mathbb{Z}$. Trata-se, obviamente, da *multiplicação* em Z, da qual destacamos as propriedades a seguir.

m_1 *Associativa*: $m(nr) = (mn)r$, para quaisquer $m, n, r \in \mathbb{Z}$. Exercício.

m_2 *Comutativa*

De fato, se $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ são elementos quaisquer de $\mathbb{Z}$, então

$$mn = \overline{(ac + bd, ad + bc)} = \overline{(ca + db, cb + da)} = nm$$

m_3 Existe *elemento neutro*: é a classe (1, 0), à qual indicaremos apenas por 1 (a justificativa para essa simplificação será vista no item 2), pois:

$$\forall\overline{(a, b)} \in \mathbb{Z} \Rightarrow \overline{(1, 0)} \cdot \overline{(a, b)} = \overline{(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)} = \overline{(a, b)}$$

m_4 *Lei do anulamento do produto*: Se m, n $\in \mathbb{Z}$ e mn = 0, então m = 0 ou n = 0.

Como já observamos anteriormente, todo elemento de $\mathbb{Z}$ pode ser representado univocamente sob uma das seguintes formas: $\overline{(a, 0)}$ ou $\overline{(0, a)}$, para algum a $\in \mathbb{N}$. Vamos supor, por exemplo, m = $\overline{(a, 0)}$ e n = $\overline{(0, b)}$. Então, por hipótese, mn = $\overline{(0, ab)} = \overline{(0, 0)}$. Daí 0 + 0 = ab + 0 ou ab = 0 (em $\mathbb{N}$), o que implica a = 0 ou b = 0. Donde m = 0 ou n = 0. Os demais casos não apresentam nenhuma novidade.

d *Distributiva*: Para quaisquer m, n, r $\in \mathbb{Z}$, m + (n + r) = (m + n) + r. Exercício.

O conjunto $\mathbb{Z}$, munido das operações introduzidas através das definições 1 e 2, mais a relação de ordem a ser introduzida no item seguinte, é chamado *conjunto dos números inteiros*. E os elementos de $\mathbb{Z}$, nessas condições, são chamados *números inteiros*.

1.4 Relação de ordem em $\mathbb{Z}$

Se m $\in \mathbb{Z}$, então m = $\overline{(a, 0)}$ ou m = $\overline{(0, a)}$, para algum a $\in \mathbb{N}$. Assim, se fizermos

$$\overline{(0, 0)} = 0 \qquad \overline{(0, 1)} = -1$$
$$\overline{(1, 0)} = +1 \qquad \overline{(0, 2)} = -2$$
$$\overline{(2, 0)} = +2 \qquad \overline{(0, 3)} = -3$$
$$\vdots \qquad\qquad \vdots$$

torna-se válido escrever

$$\mathbb{Z} = \{\ldots, -2, -1, 0, +1, +2, \ldots\}$$

Façamos $\{0, +1, +2, \ldots\} = \mathbb{Z}_+$ e $\{\ldots, -2, -1, 0\} = \mathbb{Z}_-$. Os elementos de $\mathbb{Z}_+$ se dizem *inteiros positivos* e os de $\mathbb{Z}_-$ *inteiros negativos*. Todo elemento m $\in \mathbb{Z}_+^* = \{+1, +2, +3, \ldots\}$ é chamado inteiro *estritamente positivo*; e todo m $\in \mathbb{Z}_-^* = \{\ldots, -3, -2, -1\}$ é um inteiro *estritamente negativo*.

Notemos que se m $\in \mathbb{Z}_+$ (ou $\mathbb{Z}_+^*$), então −m $\in \mathbb{Z}_-$ (ou $\mathbb{Z}_-^*$) e vice-versa. De fato, se por exemplo m = $\overline{(a, 0)}$ (logo m $\in \mathbb{Z}_+$), então −m = (0, a) (que está em $\mathbb{Z}_-$).

DEFINIÇÃO 3 Sejam m, n $\in \mathbb{Z}$. Diz-se que m *é menor que ou igual a* n e anota-se m $\leqslant$ n se

$$n = m + r$$

para algum r $\in \mathbb{Z}_+$. Neste caso também se pode escrever n $\geqslant$ m, o que se lê: "n *é maior que ou igual a* m".

Se n = m + r, onde r $\in \mathbb{Z}_+^*$, então m se diz *menor que* n. Notação: m < n. É equivalente dizer que n *é maior que* m e anotar n > m.

Em particular $0 \leqslant r$, $\forall r \in \mathbb{Z}_+$, pois r = 0 + r; e $s \leqslant 0$, $\forall s \in \mathbb{Z}_-$, já que 0 = s + (− s). Também: 0 < r, para todo r $\in \mathbb{Z}_+^*$ e r < 0 para todo r $\in \mathbb{Z}_-^*$.

Vejamos agora as propriedades mais importantes da relação $\leqslant$ sobre $\mathbb{Z}$.

o_1 *Reflexiva*: m $\leqslant$ m, $\forall$m $\in \mathbb{Z}$, pois m = m + 0 e 0 $\in \mathbb{Z}_+$.

o_2 *Anti-simétrica*: Vamos supor m $\leqslant$ n e n $\leqslant$ m. Então m = n + r_1, onde $r_1 = \overline{(a, 0)}$, para algum a $\in \mathbb{N}$, e n = m + r_2, onde $r_2 = \overline{(b, 0)}$, sendo b um conveniente elemento de $\mathbb{N}$. Então:

$$m = n + r_1 = (m + r_2) + r_1 = m + (r_1 + r_2) = m + \overline{(a + b, 0)}$$

o que implica, pela lei do cancelamento da adição:

$$\overline{(a + b, 0)} = \overline{(0, 0)}$$

Daí a + b = 0 (em $\mathbb{N}$) e portanto a = b = 0. Donde $r_1 = r_2 = 0$ e m = n.

o_3 *Transitiva*: m $\leqslant$ n e n $\leqslant$ q $\Rightarrow$ m $\leqslant$ q. (Fica como exercício.)

o_4 m $\leqslant$ n ou n $\leqslant$ m

Vamos supor m = $\overline{(a, 0)}$ e n = $\overline{(b, 0)}$. Se a $\leqslant$ b, então b = a + c, para algum c $\in \mathbb{N}$ e portanto

$$n = \overline{(b, 0)} = \overline{(a + c, 0)} = \overline{(a, 0)} + \overline{(c, 0)} = m + \overline{(c, 0)}$$

o que garante a relação m $\leqslant$ n. Se, ao contrário, ocorresse b $\leqslant$ a, então valeria n $\leqslant$ m.

O caso m = $\overline{(0, a)}$ e n = $\overline{(0, b)}$ pode ser encaminhado do mesmo modo. Finalmente, seja m = $\overline{(a, 0)}$ e n = $\overline{(0, b)}$. Então

$$m = \overline{(a, 0)} = \overline{(a + b, b)} = \overline{(0, b)} + \overline{(a + b, 0)} = n + \overline{(a + b, 0)}$$

de onde segue n $\leqslant$ m.

Uma conseqüência das considerações anteriores é que: m $\in \mathbb{Z}_-$ e n $\in \mathbb{Z}_+$ $\Rightarrow$ m $\leqslant$ n.

o_5 *Compatibilidade com a adição*: Se m $\leqslant$ n, então m + p $\leqslant$ n + p, para todo p $\in \mathbb{Z}$.

De fato, da hipótese segue que $m + r = n$, para algum $r \in \mathbb{Z}_+$. Assim, para todo $p \in \mathbb{Z}$: $n + p = (m + r) + p = (m + p) + r$. Donde: $m + p \leqslant n + p$.

o_6 *Compatibilidade com a multiplicação*: $m \leqslant n$ e $0 \leqslant p \Rightarrow mp \leqslant np$.

Por hipótese $n = m + r$, onde $r = \overline{(a, 0)}$, para algum $a \in \mathbb{N}$. Supondo $p = \overline{(b, 0)}$, como $pn = pm + pr$, onde $pr = \overline{(ab, 0)} \in \mathbb{Z}_+$, então $pm \leqslant pn$.

2. Imersão de $\mathbb{N}$ em $\mathbb{Z}$

Mostraremos agora, dentro da construção que fizemos, em que termos se pode considerar $\mathbb{N}$ como parte de $\mathbb{Z}$.

Seja $f: \mathbb{N} \to \mathbb{Z}$ definida por $f(a) = \overline{(a, 0)}$, para todo $a \in \mathbb{Z}$. Ou seja:

$$f(0) = \overline{(0, 0)} = 0$$
$$f(1) = \overline{(1, 0)} = +1$$
$$f(2) = \overline{(2, 0)} = +2$$
$$\vdots$$

Então:

- $Im(f) = \{f(a) | a \in \mathbb{N}\} = \mathbb{Z}_+ = \{0, +1, +2, +3, \ldots\}$.
- $f(a) = f(b) \Rightarrow \overline{(a, 0)} = \overline{(b, 0)} \Rightarrow a = b$, o que mostra que f é injetora.
- $f(a + b) = \overline{(a + b, 0)} = \overline{(a, 0)} + \overline{(b, 0)} = f(a) + f(b)$, $\forall a, b \in \mathbb{N}$
- $f(ab) = \overline{(ab, 0)} = \overline{(a, 0)} \cdot \overline{(b, 0)} = f(a) f(b)$, $\forall a, b \in \mathbb{N}$
- Se $a \leqslant b$, então $b = a + c$, para algum $c \in \mathbb{N}$ e portanto

$$f(b) = \overline{(b, 0)} = \overline{(a + c, 0)} = \overline{(a, 0)} + \overline{(c, 0)} = f(a) + \overline{(c, 0)}$$

o que significa que

$$f(a) \leqslant f(b)$$

Assim, no que se refere aos aspectos algébricos e à ordenação, $\mathbb{Z}_+$ é uma cópia de $\mathbb{N}$, obtida através de f. Daí porque se pode identificar $\mathbb{N}$ com $\mathbb{Z}_+$ e considerar $\mathbb{N} \subset \mathbb{Z}$. Mais especificamente, nessa identificação o número natural 0 passa a se confundir com o inteiro $0 = \overline{(0, 0)}$, o natural 1 com o inteiro $+1 = \overline{(1, 0)}$, e assim por diante. A função f considerada costuma ser chamada de *imersão* de $\mathbb{N}$ em $\mathbb{Z}$, por razões óbvias em face das propriedades que destacamos a seu respeito.

Isso posto, se $x = \overline{(a, b)} \in \mathbb{Z}$, então $x = \overline{(a, b)} = \overline{(a, 0)} + \overline{(0, b)} = \overline{(a, 0)} + [-\overline{(b, 0)}]$ e, em conseqüência da identificação feita, $x = a - b$. Logo, todo inteiro é igual à diferença (em $\mathbb{Z}$) entre dois números naturais.

Por outro lado, se $a, b \in \mathbb{N}$, levando em conta a identificação de $\mathbb{N}$ com $\mathbb{Z}_+$:

$$a - b = \overline{(a, 0)} - \overline{(b, 0)} = \overline{(a, 0)} + \overline{(0, b)} = \overline{(a, b)}$$

o que mostra que a subtração de dois números naturais é sempre possível em $\mathbb{Z}$ — e isso, no fundo, era o que se tinha em vista com a construção do conjunto dos números inteiros.

2.1 O princípio do menor inteiro

A identificação que fizemos de $\mathbb{N}$ com $\mathbb{Z}_+$ torna válida a demonstração que fizemos em 3.3 do princípio do menor inteiro:

o_7 Seja $S \subset \mathbb{Z}$, $S \neq \emptyset$. Se S admite uma cota inferior (e portanto infinitas), então S possui mínimo.

EXERCÍCIOS

352. Se $a, b, c, d \in \mathbb{Z}$, prove que:

a) $(a - b)(c - d) = (ac + bd) - (ad + bc)$

b) $(a + b)(c - d) = (ac + bc) - (ad + bd)$

353. Sejam x e y inteiros tais que $xy = 1$. Prove que $x = y = 1$ ou $x = y = -1$.

354. Prove que: $a < b + c \iff a - b < c$.

355. Se $p > 0$, prove que $a - p < a$, para todo $a \in \mathbb{Z}$.

356. Prove que: $x^2 = x \Rightarrow x = 0$ ou $x = 1$.

357. Para todo $a \in \mathbb{Z}$, mostre que

$$a - 1 = \text{máx}\{x \in \mathbb{Z} | x < a\}$$

358. Se $a < b$ e $c < d$, mostre que $a - d < b - c$.

359. Prove que: $a < b$ e $c < d \Rightarrow bc + ad < ac + bd$.

360. Mostre que, para todo $n \in \mathbb{Z}$, o conjunto $\{x \in \mathbb{Z} | n < x < n + 1\}$ é vazio.

APÊNDICE III

ARITMÉTICA MÓDULO m

Seja $m > 1$ um inteiro e indiquemos por $\mathbb{Z}_m$ o sistema completo de restos mínimos positivos, módulo m: $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. Se $x, y \in \mathbb{Z}_m$, entendemos por *soma módulo m* de x com y o resto da divisão euclidiana de $x + y$ por m. Usaremos a notação $x \overset{m}{+} y$ para indicar a soma módulo m de x com y. Por exemplo

$$6 \overset{8}{+} 7 = 5$$

pois na divisão de 13 por 8 o resto é 5.

Como o resto da divisão euclidiana de um inteiro qualquer por m está sempre em $\mathbb{Z}_m$, então a correspondência

$$(x, y) \to x \overset{m}{+} y$$

é uma lei de composição interna em $\mathbb{Z}_m$ (ou uma operação sobre $\mathbb{Z}_m$) à qual chamamos *adição módulo m*.

Para essa operação valem as propriedades:

a_1 $(x \overset{m}{+} y) \overset{m}{+} z = x \overset{m}{+} (y \overset{m}{+} z)$ (associativa)

a_2 $x \overset{m}{+} y = y \overset{m}{+} x$ (comutativa)

a_3 Existe elemento neutro: é o número 0.

a_4 Todo $a \in \mathbb{Z}_m$ tem simétrico aditivo em $\mathbb{Z}_m$: é o elemento $m - a$, pois o resto da divisão de $a + (m - a) = m$ por m é 0.

Provaremos apenas a_1, já que a demonstração das demais propriedades é imediata. Vamos supor $x \overset{m}{+} y = r_1$ $(x + y = mq_1 + r_1,\ 0 \leqslant r_1 < m)$ e $(x \overset{m}{+} y) \overset{m}{+} z = r_1 \overset{m}{+} z = r_2$ $(r_1 + z = mq_2 + r_2,\ 0 \leqslant r_2 < m)$. Daí resulta

$$(x + y) + (r_1 + z) = (mq_1 + r_1) + (mq_2 + r_2)$$

e então:

$$x + y + z = m(q_1 + q_2) + r_2 \quad (0 \leqslant r_2 < m)$$

Portanto $r_2 = (x \overset{m}{+} y) \overset{m}{+} z$ é o resto da divisão euclidiana de $x + y + z$ por m. De maneira análoga, mostra-se que $x \overset{m}{+} (y \overset{m}{+} z)$ é, também, o resto da divisão euclidiana de $x + y + z$ por m. Dessas conclusões resulta a igualdade desejada.

Para cada par de elementos $x, y \in \mathbb{Z}_m$, indicaremos por $x \overset{m}{\cdot} y$ o *produto módulo m* de x por y, assim definido:

$$x \overset{m}{\cdot} y = \text{resto da divisão euclidiana de } xy \text{ por } m$$

Obviamente a correspondência

$$(x, y) \to x \overset{m}{\cdot} y$$

define também uma lei de composição interna em $\mathbb{Z}_m$: é a chamada *multiplicação módulo m*. Para esta operação valem as seguintes propriedades:

m_1 $(x \overset{m}{\cdot} y) \overset{m}{\cdot} z = x \overset{m}{\cdot} (y \overset{m}{\cdot} z)$ (associativa)

m_2 $x \overset{m}{\cdot} y = y \overset{m}{\cdot} x$ (comutativa)

m_3 Existe elemento neutro: obviamente o número 1.

E, envolvendo adição e multiplicação, vale

d $x \overset{m}{\cdot} (y \overset{m}{+} z) = x \overset{m}{\cdot} y \overset{m}{+} x \overset{m}{\cdot} z$

ou seja, a multiplicação módulo m é distributiva em relação à adição módulo m.

As propriedades apontadas até aqui indicam que $\mathbb{Z}_m$ é, em relação à adição e à multiplicação módulo m, um modelo do que se chama em álgebra de *anel comutativo* (a qualificação "comutativo" decorre do fato de se verificar m_2)(*). Observemos que o próprio Z, em relação à adição e à multiplicação usuais, também é um anel comutativo. Vamos nos referir a $\mathbb{Z}_m$ como *anel dos inteiros módulo m* e a $\mathbb{Z}$ como *anel dos inteiros*, simplesmente. A seguir focalizaremos algumas diferenças estruturais entre os anéis $\mathbb{Z}_m$ $(m > 1)$ e $\mathbb{Z}$. Mas antes vejamos como se podem visualizar as operações num anel $\mathbb{Z}_m$, por meio de tábuas. Para $\mathbb{Z}_4$, por exemplo:

$\overset{4}{+}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\overset{4}{\cdot}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(*) Ver exercício 364.

No anel dos inteiros a relação $ab = 1$ equivale a $a = \pm 1$ e $b = \pm 1$. Isto significa que um elemento $a \in \mathbb{Z}$ tem simétrico multiplicativo (inverso) se, e somente se, $a = \pm 1$. Para estudar a mesma questão em $\mathbb{Z}_m$, façamos $U(m) = \{a \in \mathbb{Z}_m \mid \exists b \in \mathbb{Z}_m,\ a \overset{m}{\cdot} b = 1\}$. Um elemento $a \in U(m)$ é chamado *invertível* em $\mathbb{Z}_m$. Obviamente $0 \notin U(m)$, $\forall m > 1$. Se $a \in \mathbb{Z}_m$ é invertível, o elemento $b \in \mathbb{Z}_m$ tal que $a \overset{m}{\cdot} b = 1$ é único. De fato, se $a \overset{m}{\cdot} c = 1 = c \overset{m}{\cdot} a$, então

$$c = c \overset{m}{\cdot} 1 = c \overset{m}{\cdot} (a \overset{m}{\cdot} b) = (c \overset{m}{\cdot} a) \overset{m}{\cdot} b = 1 \overset{m}{\cdot} b = b$$

Esse elemento é chamado *inverso aritmético de a módulo m* e será indicado indistintamente (para todo $m > 1$) por a^*.

PROPOSIÇÃO 1 Um elemento $a \in \mathbb{Z}_m$ é invertível em $\mathbb{Z}_m$ se, e somente se, $mdc(a, m) = 1$.

Demonstração:

($\Rightarrow$) Por hipótese existe o inverso aritmético de a, módulo m: $a \overset{m}{\cdot} a^* = 1$. Daí segue que o resto da divisão de aa^* por m é 1, o que leva a $aa^* \equiv 1 \pmod m$. Logo a^* é uma solução de $ax \equiv 1 \pmod m$ e, portanto, em virtude da proposição 14, $mdc(a, m) = 1$.

($\Leftarrow$) Se $mdc(a, m) = 1$, então $ax \equiv 1 \pmod m$ admite uma solução $b \in \mathbb{Z}_m$, conforme foi visto no item 9. Daí $a \overset{m}{\cdot} b = 1$ e $b = a^*$. ■

COROLÁRIO Para que todo $a \in \mathbb{Z}_m$, $a \neq 0$, seja invertível é necessário e suficiente que m seja primo.

Demonstração:

($\Rightarrow$) Se m não fosse primo, então admitiria um divisor a, $1 < a < m$; daí $mdc(a, m) \neq 1$ (na verdade $mdc(a, m) = a$) e, devido à proposição, a não seria invertível, contrariamente à hipótese.

($\Leftarrow$) Se m é primo, então o único divisor de m em $\mathbb{Z}_m$ é 1 e portanto $mdc(a, m) = 1$, para todo $a \in \mathbb{Z}_m$, $a \neq 0$. Donde, devido à proposição, todo $a \in \mathbb{Z}_m$, $a \neq 0$, é invertível. ■

Por exemplo, se $m = 4$, como $mdc(1, 4) = mdc(3, 4) = 1$ ao passo que $mdc(0, 4) = 4$ e $mdc(2, 4) = 2$, então $U(4) = \{1, 3\}$.

Se m é primo, $U(m) = \{1, 2, \ldots, m-1\}$. Por exemplo $U(5) = \{1, 2, 3, 4\}$.

No anel $\mathbb{Z}$ vale a lei do anulamento do produto: $(\forall a, b \in \mathbb{Z})$ $(ab = 0 \Rightarrow a = 0$ ou $b = 0)$. A mesma lei não é válida em $\mathbb{Z}_6$, por exemplo, já

que $2 \overset{6}{\cdot} 3 = 0$ (também $3 \overset{6}{\cdot} 4 = 0$). Para estudar em que condições, sobre m, vale essa lei em $\mathbb{Z}_m$, seja

$$D(m) = \{a \in \mathbb{Z}_m \mid a \neq 0 \text{ e } \exists b \in \mathbb{Z}_m,\ b \neq 0,\ a \overset{m}{\cdot} b = 0\}$$

Um elemento $a \in D(m)$ é chamado *divisor próprio do zero* em $\mathbb{Z}_m$.

Por exemplo, em $\mathbb{Z}_{12}$ são divisores próprios do zero 2, 3, 4 e 6 pois $2 \overset{12}{\cdot} 6 = 3 \overset{12}{\cdot} 4 = 0$.

PROPOSIÇÃO 2 Para que $a \in \mathbb{Z}_m$, $a \neq 0$, seja um divisor próprio do zero é necessário e suficiente que $mdc(a, m) \neq 1$.

Demonstração:

($\Rightarrow$) Vamos supor, por absurdo, $mdc(a, m) = 1$. Então a é invertível em $\mathbb{Z}_m$, ou seja, existe $b \in \mathbb{Z}_m$ para o qual $a \overset{m}{\cdot} b = 1$. Mas por hipótese $a \overset{m}{\cdot} c = c \overset{m}{\cdot} a = 0$ para um conveniente $c \in \mathbb{Z}_m$, $c \neq 0$. Daí

$$c = c \overset{m}{\cdot} 1 = c \overset{m}{\cdot} (a \overset{m}{\cdot} b) = (c \overset{m}{\cdot} a) \overset{m}{\cdot} b = 0 \overset{m}{\cdot} b = 0$$

o que é absurdo.

($\Leftarrow$) Como $mdc(a, m) \neq 1$, então existe um primo $p > 1$ tal que $p \mid a$ e $p \mid m$. Não se pode ter $p = m$ pois isto levaria à relação $m \mid a$, a qual não pode ocorrer visto que $a \in \mathbb{Z}_m$. Logo $m = pq$, onde $1 < p, q < m$. Como o resto da divisão de $pq = m$ por m é 0, então $p \overset{m}{\cdot} q = 0$ e portanto $p, q \in D(m)$.
Mas como $p \mid a$, então $a = ps$, onde s é um conveniente elemento de $\mathbb{Z}_m$. Daí $aq = (pq)s$ e então

$$a \overset{m}{\cdot} q = (p \overset{m}{\cdot} q) \overset{m}{\cdot} s = 0$$ ■

o que mostra que $a \in D(m)$.

COROLÁRIO Um anel $\mathbb{Z}_m$ não possui divisores próprios do zero se, e somente se, m é primo.

Demonstração:

$\mathbb{Z}_m$ não possui divisores próprios do zero se, e somente se, $mdc(a, m) = 1$, $\forall a \in \mathbb{Z}_m$, $a \neq 0$. Mas $mdc(a, m) = 1$, $\forall a \in \mathbb{Z}_m$, $a \neq 0$, equivale a dizer que todo $a \in \mathbb{Z}_m$, $a \neq 0$, é invertível. O que ocorre, segundo o corolário da proposição anterior, quando e somente quando m é primo. ■

Do que foi exposto até aqui decorre a seguinte partição

$$\mathbb{Z}_m = \{0\} \cup U(m) \cup D(m)$$

onde $D(m) = \varnothing$ se m é primo.

Por exemplo, para $\mathbf{Z}_8$:

$$\mathbf{Z}_8 = \{0\} \cup U(8) \cup D(8)$$

onde $U(8) = \{1, 3, 5, 7\}$ e $D(8) = \{2, 4, 6\}$.

Exemplos:

1) Voltemos a examinar a congruência linear $ax \equiv b \pmod m$, onde $a \neq 0$ e $mdc(a, m) = 1$.

Se a^* é o inverso aritmético de a, módulo m, então $aa^* \equiv 1 \pmod m$ e portanto

$$(aa^*)b = a(a^*b) \equiv b \pmod m$$

o que mostra que a^*b é uma solução particular da congruência dada.

Assim, o conjunto das soluções de $ax \equiv b \pmod m$ onde $a \neq 0$ e $mdc(a, m) = 1$ é:

$$\{a^*b + mt \mid t \in \mathbf{Z}\}$$

Por exemplo, no caso da congruência $5x \equiv 19 \pmod{23}$, como $5^* = 14$ (pois $5 \overset{23}{\cdot} 14 = 1$) e como $14 \cdot 19 = 266 \equiv 13 \pmod{23}$, então pode-se tomar o 13 como solução particular da congruência dada, cuja solução geral é:

$$x \equiv 13 \pmod{23}$$

2) Seja $a \in \mathbf{Z}_m$. Para todo inteiro $r \geqslant 1$ a potência r-ésima de a em $\mathbf{Z}_m$ se define da maneira usual:

$a^1 = a$

$a^r = a \overset{m}{\cdot} a \overset{m}{\cdot} \ldots \overset{m}{\cdot} a$ (r fatores), se $r > 1$. (Não estamos distinguindo a notação de potência em $\mathbf{Z}_m$ daquela em $\mathbf{Z}$, para não sobrecarregar a notação.)

Nessas condições, se $a \in \mathbf{Z}_m$ e $mdc(a, m) = 1$, a ordem de a, módulo m, é o menor inteiro $d > 0$ para o qual se verifica a igualdade $a^d = 1$ (em $\mathbf{Z}_m$).

Assim, por exemplo, em $\mathbf{Z}_4 = \{0, 1, 2, 3\}$, como

$$3^1 = 3 \text{ e } 3^2 = 1 \quad (\text{pois } 3 \cdot 3 \equiv 1 \pmod 4)$$

então, a ordem de 3, módulo 4, é 2.

Em $\mathbf{Z}_m$ então

$$a^{\varphi(m)} = 1$$

para todo a tal que $mdc(a, m) = 1$. Em particular, se p é primo, então

$$a^{p-1} = 1 \quad (\forall a \in \mathbf{Z}_p;\ a \neq 0)$$

pois todo $a \in \mathbf{Z}_p$, $a \neq 0$, é primo com p neste caso. Isso significa que para todo primo $p > 1$ a equação

$$x^{p-1} = 1$$

tem $p - 1$ raízes em $\mathbf{Z}_p$: todos os elementos não nulos de $\mathbf{Z}_p$.

EXERCÍCIOS

361. Resolva, com o uso do inverso aritmético do coeficiente de x, as seguintes congruências lineares:

a) $3x \equiv 7 \pmod{23}$

b) $8x \equiv 2 \pmod{30}$

c) $5x \equiv 3 \pmod{19}$

d) $9x \equiv -1 \pmod{17}$

362. Seja $m > 1$ um inteiro. Para cada $a \in \mathbf{Z}_m$ fixado, mostre que $f = \mathbf{Z}_m \to \mathbf{Z}_m$ definida por $f(x) = x \overset{m}{+} a$ é bijetora.

Resolução:

i Se $x, y \in \mathbf{Z}_m$ e $x \overset{m}{+} a = y \overset{m}{+} a$, adicionando (módulo m) o simétrico aditivo $p - a$ de a a ambos os membros da igualdade:

$$(x \overset{m}{+} a) \overset{m}{+} (p - a) = (y \overset{m}{+} a) \overset{m}{+} (p - a)$$

Daí

$$x \overset{m}{+} [a \overset{m}{+} (p - a)] = y \overset{m}{+} [a \overset{m}{+} (p - a)]$$

ou

$$x \overset{m}{+} 0 = y \overset{m}{+} 0$$

de onde resulta $x = y$; logo f é injetora.

ii Dado $y \in \mathbf{Z}_m$, tomando $x = y \overset{m}{+} a'$ ($a' = p - a$ = simétrico aditivo de a), então $x \in \mathbf{Z}_m$ e $f(x) = (y \overset{m}{+} a') \overset{m}{+} a = y \overset{m}{+} (a' \overset{m}{+} a) = y \overset{m}{+} 0 = y$; donde f é sobrejetora.

363. A *criptografia* objetiva, em suma, a codificação de mensagens. Para tanto são usadas uma chave de transmissão através da qual a mensagem é codificada e uma chave de recepção para decodificá-la. Nos casos mais simples essas chaves são iguais.

Um dos sistemas criptográficos mais antigos e simples é a chamada "cifra de César" (a razão do nome é que Júlio César a usava). A cifra de César baseia-se na propriedade exposta no exercício anterior.

Imaginemos as 26 letras usuais e o espaço (entre duas palavras) associados aos elementos de $\mathbf{Z}_{27}$ conforme o quadro:

espaço ⊔	A	B	C	...	J	K	L	...	X	Y	Z
0	1	2	3	...	10	11	12	...	24	25	26

Fixado um elemento $a \in \mathbb{Z}_m$ (a é a chave do código — de transmissão e de recepção), a aplicação $x \xrightarrow{f} x \overset{27}{+} a$ permuta os elementos de $\mathbb{Z}_{27}$ e, conseqüentemente, os elementos do conjunto formado pelo símbolo do espaço e as 26 letras. Dessa forma cada mensagem se transforma em código; o fato de f ser bijetora garante que mensagens diferentes são codificadas de maneira diferente e, ainda, a possibilidade da decodificação.

Vejamos, por exemplo, como codificar a frase "eu vou", usando como chave a = 15.

$$\begin{array}{lllllll}
E & \to & 5 & \to & 5 \overset{27}{+} 15 = 20 & \to & T \\
U & \to & 21 & \to & 21 \overset{27}{+} 15 = 9 & \to & I \\
\sqcup & \to & 0 & \to & 0 \overset{27}{+} 15 = 15 & \to & O \\
V & \to & 22 & \to & 22 \overset{27}{+} 15 = 10 & \to & J \\
O & \to & 15 & \to & 15 \overset{27}{+} 15 = 3 & \to & C \\
U & \to & 21 & \to & 21 \overset{27}{+} 15 = 9 & \to & I
\end{array}$$

Portanto o código para a frase dada é "TIOJCI".

Para decodificar, por exemplo, G X A, considerando que o simétrico aditivo de 15 é 12 (mantendo, portanto, a chave a = 15), procede-se assim:

$$\begin{array}{lllllll}
G & \to & 7 & \to & 7 \overset{27}{+} 12 = 19 & \to & S \\
X & \to & 24 & \to & 24 \overset{27}{+} 12 = 9 & \to & I \\
A & \to & 1 & \to & 1 \overset{27}{+} 12 = 13 & \to & M
\end{array}$$

Logo, a mensagem era "sim".

Isto posto:

a) Codifique "Teoria dos números" usando a = 5 como chave.

b) Se a chave usada foi a = 12, decodifique a mensagem:

O M Y A ⊔ D L Z F Y Q C U O ⊔ D

364. Como já foi esboçado neste Apêndice, um *anel comutativo* é constituído de um conjunto $A \neq \emptyset$, uma "adição" $(x, y) \to x + y$ e uma "multiplicação" $(x, y) \to xy$ sobre A, de modo que: $\mathbf{a_1}$ $(a + b) + c = a + (b + c)$, $\forall a, b, c \in A$; $\mathbf{a_2}$ $a + b = b + a$, $\forall a, b \in A$; $\mathbf{a_3}$ existe elemento neutro para a adição, ou seja, um elemento $0 \in A$ tal que $a + 0 = a$, $\forall a \in A$; $\mathbf{a_4}$ para todo $a \in A$ existe $a' \in A$ tal que $a + a' = e$ (a' é o oposto ou simétrico aditivo de a) $\mathbf{m_1}$ $a(bc) = (ab)c$, $\forall a, b, c \in A$; $\mathbf{m_2}$ existe elemento neutro para a multiplicação, ou seja, um elemento $1 \in A$ tal que $a \cdot 1 = a$, $\forall a \in A$; $\mathbf{m_3}$ $ab = ba$, $\forall a, b \in A$; **d** $a(b + c) = ab + ac$, $\forall a, b, c \in A$.

São exemplos de anéis, como já vimos, $\mathbb{Z}$ e $\mathbb{Z}_m$ ($\forall m > 1$).

Num anel comutativo A a soma e o produto de n elementos $a_1, a_2, \ldots, a_n \in A$ ($n > 2$), bem como a potência enésima de $a \in A$ ($n \geq 1$) se definem generalizando os conceitos respectivos em $\mathbb{Z}$. Assim, são definidos por recorrência do seguinte modo:

$$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n \qquad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n$$

e

$$a^1 = a, \; a^n = a^{n-1} \cdot a \quad (n > 1)$$

Isso posto, provemos a chamada *fórmula do binômio de Newton* para um anel comutativo A qualquer:

"Se x e y são elementos não nulos de um anel comutativo (ou seja, x e y são diferentes do elemento neutro da adição de A) então, para todo $n \geq 1$, vale a relação

$$(x + y)^n = \sum_{p=0}^{n} \binom{n}{p} x^{n-p} y^p \quad (*)$$

onde

$$\binom{n}{p} = \frac{n!}{p!\,(n-p)!} \quad (0 \leq p \leq n)\text{"}$$

Observemos que, por definição, $a^0 = 1$ (elemento neutro da multiplicação) para todo $a \neq 0$ e $0! = 1$.

Resolução:

i Provemos primeiro a *relação de Stifel* para os coeficientes binomiais que figuram na fórmula do binômio, ou seja

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1} \quad (1 \leq r \leq n-1)$$

De fato:

$$\binom{n-1}{r} + \binom{n-1}{r-1} = \frac{(n-1)!}{r!\,(n-r-1)!} + \frac{(n-1)!}{(r-1)!\,(n-r)!} =$$

$$= \frac{(n-1)!}{r(r-1)!\,(n-r-1)!} + \frac{(n-1)!}{(r-1)!\,(n-r)\,(n-r-1)!} =$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r-1)!}\left(\frac{1}{r} + \frac{1}{n-r}\right) =$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r-1)!} \quad \frac{n}{r(n-r)} = \frac{n!}{r!\,(n-r)!} = \binom{n}{r}$$

ii A fórmula do binômio será provada por indução sobre n.

$n = 1$:

$(x + y)^1 = x + y$

$$\sum_{p=0}^{1} \binom{1}{p} x^{1-p} y^p = x^{1-0} y^0 + x^0 y^1 = x + y$$

Logo, a fórmula vale para $n = 1$.

Seja $n \geqslant 2$ e suponhamos:

$$(x + y)^{n-1} = \sum_{p=0}^{n-1} \binom{n-1}{p} x^{n-1-p} y^p$$

Multiplicando por $x + y$ a relação anterior:

$$(x + y)^n = \sum_{p=0}^{n-1} \binom{n-1}{p} x^{n-p} y^p + \sum_{p=0}^{n-1} \binom{n-1}{p} x^{n-1-p} y^{p+1}$$

Ora, se r é um inteiro tal que $0 < r < n$, então no segundo membro da relação anterior há dois termos cuja parte literal é $x^{n-r} y^r$: o primeiro se obtém para $p = r$ no primeiro somatório, sendo seu coeficiente o número $\binom{n-1}{r}$, e o outro se obtém para $p = r - 1$ no segundo somatório, sendo seu coeficiente o número $\binom{n-1}{r-1}$. Logo o coeficiente de $x^{n-r} y^r$ em $(x + y)^n$ é:

$$\binom{n-1}{r} + \binom{n-1}{r-1} = \binom{n}{r}$$

Então:

$$(x + y)^n = \binom{n-1}{0} x^n y^0 + \sum_{r=1}^{n-1} \binom{n}{r} x^{n-r} y^r + \binom{n-1}{n-1} x^0 y^n =$$

$$= \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$$

posto que

$$\binom{n-1}{0} = \binom{n}{0} \quad \text{e} \quad \binom{n-1}{n-1} = \binom{n}{n}$$

CAPÍTULO IV

OS NÚMEROS RACIONAIS

1. Introdução

Sempre que a divisão de um inteiro por outro não era exata, os egípcios antigos, já por volta do ano 2000 a.C., usavam frações para exprimir o resultado. E usavam também frações para operar com seu sistema de pesos e medidas.

Contudo, por razões difíceis de explicar, com exceção das frações $\frac{2}{3}$ e $\frac{3}{4}$, às vezes, os egípcios usavam apenas *frações unitárias*, ou seja, frações cujo numerador é 1. Por exemplo, no problema 24 do papiro Rhind (cerca de 1700 a.C.) no qual o escriba pede que se efetue a divisão de 19 por 8, a resposta é dada, usando a nossa notação, por:

$$2 + \frac{1}{4} + \frac{1}{8}$$

Embora os egípcios não adotassem sempre o mesmo procedimento, pode-se mostrar que toda fração entre 0 e 1 é soma de frações unitárias, o que representa uma garantia teórica para essa opção.

Aliás, o uso das frações unitárias, além de não ficar confinado ao Egito antigo, se estendeu por vários séculos. Basta dizer que Fibonacci, no seu já citado *Liber abaci*, escrito no século XIII d.C. (cap. II, item 11), não só as usava como fornecia tabelas de conversão das frações comuns para unitárias. É que, embora uma das finalidades dessa obra fosse divulgar os numerais indo-arábicos e a notação decimal posicional, Fibonacci não chegou a perceber a grande vantagem deste sistema: sua aplicabilidade para exprimir frações. Por exemplo:

$$\frac{1}{4} = 0{,}25.$$

Mas convém registrar que os babilônios, 2 000 anos antes de Cristo, apesar de algumas ambigüidades, decorrentes de não contarem com um sím-

bolo para o zero e outro para a separatriz, conseguiram estender o princípio posicional às frações no seu sistema de base 60. Por exemplo, o numeral

YY

que, como já vimos no capítulo I, poderia representar o inteiro $1 + 1 \cdot 60 = 61$, também poderia ser uma representação de

$$1 + \frac{1}{60}$$

Na verdade o uso da *forma decimal* para representar frações, tal como em $\frac{1}{4} = 0{,}25$, somente começaria a vingar após a publicação, em 1585, de um pequeno texto de Simon Stevin (1548-1620) intitulado *De thiende* (O décimo). Embora a essa altura a forma decimal já não constituísse uma novidade para os especialistas, esse trabalho de Stevin alcançou grande popularidade e conseguiu seu intento, que era ensinar a "como efetuar, com facilidade nunca vista, todos os cálculos necessários entre os homens, por meio de inteiros sem frações". A notação inicialmente usada por Stevin acabou sendo melhorada com o emprego da vírgula ou do ponto como separatriz decimal, conforme sugestão de John Napier (1550-1617), feita em 1617.

2. A divisão em $\mathbb{Z}$

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Se a é múltiplo de b, então existe um único $c \in \mathbb{Z}$ de maneira que $a = bc$. Este elemento c é chamado *quociente* de a por b e costuma ser indicado por:

$$c = \frac{a}{b} \text{ ou } c = a : b$$

A operação que a cada par (a, b), nas condições expostas, associa $c = a : b$ é a *divisão em* $\mathbb{Z}$. Portanto a divisão em $\mathbb{Z}$ só está definida em

$$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0 \text{ e } b|a\}$$

Mas certas questões corriqueiras ao homem há milênios, como a citada no item anterior de dividir 19 por 8, embora envolvendo só números inteiros, não admitem uma resposta no âmbito de $\mathbb{Z}$. É coerente indicar essa resposta por $\frac{19}{8}$, uma vez que se o primeiro número fosse 16 ela se exprimiria por $2 = \frac{16}{8}$. Cumpre então ampliar $\mathbb{Z}$ convenientemente de maneira

a poder abarcar todos os quocientes $\frac{a}{b}$ ($a, b \in \mathbb{Z}$, $b \neq 0$) que possam surgir de questões da mesma natureza da que acabamos de lembrar.

Essa ampliação, tal como no caso de $\mathbb{N}$ para $\mathbb{Z}$, pode ser feita de duas maneiras: elementarmente, agregando-se a $\mathbb{Z}$ os novos quocientes e definindo no conjunto resultante as operações e a relação de ordem convenientes; ou formalmente, construindo a partir de $\mathbb{Z}$ um novo conjunto, com os requisitos desejados, mas de tal modo que uma de suas partes possa ser identificada plenamente com $\mathbb{Z}$. É claro que historicamente o caminho seguido foi o primeiro.

Optamos por fazer a construção formal do conjunto dos números racionais (a ampliação pretendida de $\mathbb{Z}$) já no corpo do capítulo porque, além de um pouco menos penosa que a de $\mathbb{Z}$, é mais difundida, mesmo em nível elementar, e portanto trata-se de algo certamente mais familiar ao leitor.

3. Números racionais: construção, operação e relação de ordem

Seja $\mathbb{Z}^* = \{m \in \mathbb{Z} \mid m \neq 0\}$ e consideremos sobre $\mathbb{Z} \times \mathbb{Z}^* = \{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{Z}^*\}$ a relação $\sim$ definida por

$$(m, n) \sim (p, q) \text{ se, e somente se, } mq = np$$

Para $\sim$ valem as três propriedades que caracterizam uma relação de equivalência, ou seja:

i $(m, n) \sim (m, n)$, para todo $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$ (reflexiva)
ii $(m, n) \sim (p, q) \Rightarrow (p, q) \sim (m, n)$ (simétrica)
iii $(m, n) \sim (p, q)$ e $(p, q) \sim (r, s) \Rightarrow (m, n) \sim (r, s)$ (transitiva)

Verifiquemos **iii** já que **i** e **ii** decorrem diretamente da definição de $\sim$. Por hipótese: $mq = np$ e $ps = qr$. Multiplicando a primeira dessas igualdades por s e a segunda por n, resulta: $mqs = nps$ e $nps = nqr$. Daí, $mqs = nqr$ e portanto, cancelando q, o que é possível pois $q \in \mathbb{Z}^*$, obtém-se $ms = nr$. Donde $(m, n) \sim (r, s)$.

Logo a relação $\sim$ determina sobre $\mathbb{Z} \times \mathbb{Z}^*$ uma partição em classes de equivalência. Para cada par $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$, a classe de equivalência à qual esse elemento pertence será indicada por $\frac{m}{n}$. Ou seja:

$$\frac{m}{n} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* \mid (x, y) \sim (m, n)\} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* \mid nx = my\}$$

Por exemplo:

$$\frac{1}{2} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* \mid 2x = y\} = \{(1, 2); (-1, -2); (2, 4); (-2, -4); \ldots\}$$

Devido à propriedade reflexiva, é claro que $(m, n) \in \frac{m}{n}$, para todo $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$. Além disso, como

$$\frac{m}{n} = \frac{r}{s} \iff (m, n) \sim (r, s)$$

(resultado da teoria das relações de equivalência), então:

$$\frac{m}{n} = \frac{r}{s} \iff ms = nr$$

Por exemplo:

$$\frac{1}{2} = \frac{-1}{-2} = \frac{2}{4} = \frac{-2}{-4} = \dots$$

O conjunto quociente de $\mathbb{Z} \times \mathbb{Z}^*$ por $\sim$, ou seja, o conjunto de todas as classes de equivalência determinada por $\sim$ sobre $\mathbb{Z} \times \mathbb{Z}^*$, será designado por $\mathbb{Q}$. Logo:

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid (m, n) \in \mathbb{Z} \times \mathbb{Z}^* \right\}$$

Assim, cada $a \in \mathbb{Q}$ admite infinitas representações $\frac{m}{n}$ $(m \in \mathbb{Z};\ n \in \mathbb{Z}^*)$. Em cada uma delas m é o *numerador* e n o *denominador*. Dois elementos a, $b \in \mathbb{Q}$ sempre admitem representações de denominadores iguais. De fato, se $a = \frac{m}{n}$ e $b = \frac{r}{s}$, então

$$\frac{m}{n} = \frac{ms}{ns} \text{ e } \frac{r}{s} = \frac{nr}{ns}$$

pois $m(ns) = n(ms)$ e $r(ns) = s(nr)$.

Os elementos de $\mathbb{Q}$ são chamados *números racionais* desde que se definam adição, multiplicação e relação de ordem, conforme o faremos nos itens seguintes.

3.1 Adição em Q

DEFINIÇÃO 1 Sejam $a = \frac{m}{n}$ e $b = \frac{r}{s}$ elementos de $\mathbb{Q}$. Chama-se *soma* de a com b e indica-se por a + b o elemento de $\mathbb{Q}$ definido da seguinte maneira:

$$a + b = \frac{ms}{ns} + \frac{nr}{ns} = \frac{ms + nr}{ns}$$

Mostremos que a soma a + b independe dos pares ordenados escolhidos para definir a e b. De fato, se $a = \frac{m}{n} = \frac{m'}{n'}$ e $b = \frac{r}{s} = \frac{r'}{s'}$, então

$$mn' = nm' \text{ e } rs' = sr'$$

Multiplicando a primeira dessas igualdades por ss' e a segunda por nn' e somando membro a membro as relações obtidas

$$msn's' + rns'n' = nsm's' + nsr'n'$$

ou seja

$$(ms + rn)n's' = ns(m's' + r'n')$$

o que garante

$$\frac{ms + rn}{ns} = \frac{m's' + r'n'}{n's'}$$

Portanto a correspondência

$$(a, b) \to a + b,$$

conforme a definição 1, é uma aplicação e, portanto, trata-se de uma operação sobre $\mathbb{Q}$, à qual chamamos *adição em $\mathbb{Q}$*.

Para a adição em $\mathbb{Q}$ valem as seguintes propriedades:

a_1 $(a + b) + c = a + (b + c)$, $\forall a, b, c \in \mathbb{Q}$ (associativa)

a_2 $a + b = b + a$, $\forall a, b, \in \mathbb{Q}$ (comutativa)

a_3 Existe elemento neutro: é a classe de equivalência $\frac{0}{1} = \frac{0}{2} = \dots$, que indicamos por 0 apenas. De fato

$$\frac{m}{n} + \frac{0}{1} = \frac{m \cdot 1 + 0 \cdot n}{n \cdot 1} = \frac{m \cdot 1}{n \cdot 1} = \frac{m}{n}$$

para todo $\frac{m}{n} \in \mathbb{Q}$.

a_4 Todo $a \in \mathbb{Q}$ admite simétrico aditivo (oposto) em $\mathbb{Q}$: se $a = \frac{m}{n}$, então $-a = \frac{-m}{n}$, pois:

$$\frac{m}{n} + \frac{-m}{n} = \frac{mn + (-m)n}{nn} = \frac{0}{nn} = 0$$

Usaremos a notação $\mathbb{Q}^* = \{a \in \mathbb{Q} \mid a \neq 0\}$.

DEFINIÇÃO 2 Se a, b $\in \mathbb{Q}$, denomina-se *diferença* entre a e b, e indica-se por a − b, o seguinte elemento de $\mathbb{Q}$:

$$a - b = a + (-b)$$

Como $(-b) \in \mathbb{Q}$, para todo $b \in \mathbb{Q}$, então

$$(a, b) \rightarrow a - b$$

é uma operação sobre $\mathbb{Q}$, à qual chamamos *subtração* em $\mathbb{Q}$.

Tal como ocorre em **Z** (cap. III, 3.1), valem em $\mathbb{Q}$ as seguintes propriedades, envolvendo a idéia de oposto e de subtração:

- $-(a + b) = -a - b$
- $(a - b) + b = a$
- $a + x = b \iff x = b - a$
- $a + b = a + c \Rightarrow b = c$

Para demonstrá-las, o procedimento pode ser o mesmo usado para **Z**.

3.2 Multiplicação em $\mathbb{Q}$

DEFINIÇÃO 3 Chamamos *produto* de $a = \frac{m}{n} \in \mathbb{Q}$ por $b = \frac{r}{s} \in \mathbb{Q}$ o elemento

$$ab = a \cdot b = \frac{mr}{ns} \in \mathbb{Q}$$

o qual, pode-se mostrar (tal como foi feito para a soma em 3.1), não depende das particulares representações tomadas para a e b.

A *multiplicação* em $\mathbb{Q}$ é a operação definida por

$$(a, b) \longrightarrow ab$$

para quaisquer $a, b \in \mathbb{Q}$.

Valem as seguintes propriedades:

$\mathbf{m_1}$ $a(bc) = (ab)c$, $\forall a, b, c \in \mathbb{Q}$ (associativa)

$\mathbf{m_2}$ $ab = ba$, $\forall a, b, \in \mathbb{Q}$ (comutativa)

$\mathbf{m_3}$ Existe elemento neutro: é a classe

$$\frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \ldots$$

que indicamos simplesmente por 1. De fato:

$$\frac{m}{n} \cdot \frac{1}{1} = \frac{m \cdot 1}{n \cdot 1} = \frac{m}{n}$$

para todo $\frac{m}{n} \in \mathbb{Q}$

$\mathbf{m_4}$ Todo $a \in \mathbb{Q}$, $a \neq 0$, admite simétrico multiplicativo (inverso): se

$$a = \frac{m}{n}$$

então $m \neq 0$ e daí $\frac{n}{m} \in \mathbb{Q}$ e portanto

$$\frac{m}{n} \cdot \frac{n}{m} = \frac{mn}{nm} = 1$$

Indicando por a^{-1}, como é praxe, o inverso de a, então

$$a = \frac{m}{n},\ a \neq 0 \ \Rightarrow\ a^{-1} = \frac{n}{m}$$

Disso decorre também que se $a \neq 0$:

$$(a^{-1})^{-1} = \left(\frac{n}{m}\right)^{-1} = \frac{m}{n} = a$$

Outro fato importante no que se refere aos inversos é que se a e b são elementos não nulos:

$$(ab)^{-1} = a^{-1}b^{-1}$$

De fato, como

$$(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = 1$$

então efetivamente $a^{-1}b^{-1}$ é o inverso de ab.

d A multiplicação é distributiva em relação à adição:

$$a(b + c) = ab + ac,\ \forall a, b, c \in \mathbb{Q}$$

Nota (sobre a noção de *corpo*): Suponhamos que sobre um conjunto $K \neq \varnothing$ estejam definidas uma "adição" e uma "multiplicação", a primeira (segunda) associando a cada par de elementos $a, b \in K$ um único elemento, também de K, que se indica por a + b (respectivamente ab ou a · b) chamado soma de a com b (respectivamente, produto de a por b), de modo que:

i $(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$, para quaisquer $a, b, c \in K$ (valem as propriedades associativas).

ii $a + b = b + a$ e $ab = ba$, para quaisquer $a, b \in K$ (valem as propriedades comutativas).

iii Existem elementos $u, e \in K$ de modo que $a + u = a$ ($\forall a \in K$) e $a \cdot e = a$ ($\forall a \in K$), ou seja, existem elementos neutros para ambas as operações. Para facilitar a notação é comum fazer $u = 0$ e $e = 1$.

iv Para todo $a \in K$ existe $a' \in K$, de modo que $a + a' = 0$ (todo $a \in K$ admite simétrico aditivo a'); e para todo $a \in K^* = K - \{0\}$ existe $a'' \in K$, para o qual se verifica $aa'' = 1$ (a'' é o simétrico multiplicativo de a). A notação usual para os simétricos é: $a' = -a$ e $a'' = a^{-1}$.

v para quaisquer $a, b, c \in K$

$$a(b + c) = ab + ac$$

(a multiplicação é distributiva em relação à adição).

Nessas condições diz-se que sobre K está definida uma *estrutura de corpo* ou, simplesmente, que K é um corpo. Essas designações são tiradas da álgebra. Note-se que todo corpo é um anel comutativo (ver exercício 364).

Logo, $\mathbb{Q}$ é um exemplo de corpo. Outro exemplo já visto neste texto é o do conjunto $\mathbb{Z}_m$, para m primo, com a adição e a multiplicação módulo m (Apêndice III, cap. III). No capítulo V estudaremos o corpo dos números reais.

Convém ainda destacar os seguintes resultados para a multiplicação em $\mathbb{Q}$:

- $a(b - c) = ab - ac$
- $a \cdot 0 = 0$
- $a(-b) = (-a)b = -(ab)$
- $(-a)(-b) = ab$

Todas essas propriedades podem ser provadas como as respectivas de $\mathbb{Z}$ (cap. III, 3.2).

- $ab = 0 \Rightarrow a = 0$ ou $b = 0$

Prova: Supondo $a \neq 0$, então de $ab = 0$ decorre $a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Como $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$, então $b = 0$.

- $(ab = ac$ e $a \neq 0) \Rightarrow b = c$

Prova: $ab = ac \Rightarrow ab + [-(ac)] = 0 \Rightarrow$
$\Rightarrow ab + a(-c) = 0 \Rightarrow a(b - c) = 0 \overset{(a \neq 0)}{\Rightarrow} b - c = 0 \Rightarrow b = c.$

Na verdade, as duas últimas propriedades (lei do anulamento do produto e lei do cancelamento da multiplicação) são logicamente equivalentes entre

si. A demonstração que acabamos de fazer mostra que a última lei citada é conseqüência da primeira. Quanto à recíproca, supondo $a \neq 0$ e $ab = 0$, como $0 = a \cdot 0$, então $ab = a \cdot 0$ e, pela hipótese, $b = 0$.

- Para todo $a \in \mathbb{Q}^*$: $ax = b \iff x = a^{-1}b$.

$\Rightarrow$ Da hipótese segue que $a^{-1}(ax) = a^{-1}b$. Mas $a^{-1}(ax) = (a^{-1}a)x = 1 \cdot x = x$. Logo $x = a^{-1}b$.

$\Leftarrow$ Como $x = a^{-1}b$, então

$$ax = a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b$$

DEFINIÇÃO 4 Entendemos por *divisão em* $\mathbb{Q}$ a operação de $\mathbb{Q} \times \mathbb{Q}^*$ em $\mathbb{Q}$ definida por

$$(a, b) \rightarrow ab^{-1}$$

O elemento ab^{-1} é chamado *quociente* de a por b e pode ser indicado por $a : b$.

Por exemplo, se $a = \frac{2}{3}$ e $b = \frac{1}{5}$, então:

$$a : b = \frac{2}{3} \left(\frac{1}{5}\right)^{-1} = \frac{2}{3} \cdot \frac{5}{1} = \frac{10}{3}$$

Para a divisão em $\mathbb{Q}$ vale a seguinte propriedade: se $a, b, c \in \mathbb{Q}$ e $c \neq 0$, então:

$$(a + b) : c = a : c + b : c$$

De fato, se $c = \frac{r}{s}$ ($r, s \in \mathbb{Z}^*$), então:

$$(a+b) : c = (a+b) \cdot \frac{s}{r} = a \cdot \frac{s}{r} + b \cdot \frac{s}{r} = a : \frac{r}{s} + b : \frac{r}{s} = a : c + b : c.$$

3.3 Somas e produtos de mais de dois elementos em $\mathbb{Q}$

A maneira de estender o conceito de soma e o de produto para n números racionais ($n > 2$) segue o procedimento de sempre em situações análogas. Se $a_1, a_2, \ldots, a_n \in \mathbb{Q}$ ($n > 2$), por recorrência definem-se

$$a_1 + a_2 + \ldots + a_n = (a_1 + a_2 + \ldots + a_{n-1}) + a_n \quad \text{e} \quad a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n$$

ou, com os símbolos usuais de somatório e produtório:

$$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n \quad \text{e} \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n$$

Se fizermos, para n = 1,

$$\sum_{i=1}^{n} a_i = a_1 \quad e \quad \prod_{i=1}^{n} a_i = a_1$$

torna-se mais fácil expressar (e até provar) algumas propriedades envolvendo n números racionais ($n \geq 1$). Destaquemos a generalização da propriedade distributiva da multiplicação em relação à adição (cuja demonstração é análoga à que foi feita no cap. III, 4.3, para $\mathbb{N}$): se $a, b_1, b_2, \ldots, b_n \in \mathbb{Q}$ ($n \geq 1$), então

$$a\left(\sum_{i=1}^{n} b_i\right) = \sum_{i=1}^{n} (ab_i)$$

Mas também podemos generalizar propriedades mais específicas de $\mathbb{Q}$. Por exemplo, se $a_1, a_2, \ldots, a_n \in \mathbb{Q}^*$, então

$$\left(\prod_{i=1}^{n} a_i\right)^{-1} = \prod_{i=1}^{n} a_i^{-1}$$

ou seja, "o inverso de um produto de elementos não nulos é o produto dos inversos". De fato:

$$n = 1: \left(\prod_{i=1}^{n} a_i\right)^{-1} = a_1^{-1} = \prod_{i=1}^{n} a_i^{-1}$$

Vamos supor $\left(\prod_{i=1}^{r} a_i\right)^{-1} = \prod_{i=1}^{r} a_i^{-1} \quad (r \geq 1)$

$$n = r + 1: \prod_{i=1}^{r+1} a_i^{-1} = \left(\prod_{i=1}^{r} a_i^{-1}\right) a_{r+1}^{-1} \overset{(*)}{=}$$

$$= \left(\prod_{i=1}^{r} a_i\right)^{-1} \cdot a_{r+1}^{-1} \overset{(**)}{=} \left[\left(\prod_{i=1}^{r} a_i\right) \cdot a_{r+1}\right]^{-1} = \left(\prod_{i=1}^{r+1} a_i\right)^{-1}$$

Note-se que em (*) usamos a hipótese de indução e que em (**) o fato de o resultado ser válido para n = 2, o que já havia sido demonstrado em 3.2.

Exemplo 1: Seja $a \in \mathbb{Q}$, $a \neq 0$. Para um inteiro m qualquer, entende-se por *potência* m-ésima de a o elemento $a^m \in \mathbb{Q}$ assim definido:

Se $m \geq 0$, recursivamente por

$$a^0 = 1$$
$$a^{m+1} = a^m \cdot a, \text{ sempre que } m \geq 0.$$

Se $m < 0$, então:

$$a^m = (a^{-1})^{-m}$$

Essa definição implica que, quando $m > 0$, então $a^m = a \cdot a \ldots a$ (m fatores).

Mostremos que $a^m \cdot a^n = a^{m+n}$ para todo $a \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$ e quaisquer $m, n \in \mathbb{Z}$.

Primeiro notemos que mesmo quando $n < 0$ vale $a^n \cdot a = a^{n+1}$ De fato, se $n < 0$, então $-n = p > 0$ e, portanto:

$$a^n \cdot a = (a^{-1})^p \cdot a = [(a^{-1})^{p-1} \cdot a^{-1}] \cdot a = (a^{-1})^{p-1} \cdot (a^{-1} \cdot a) =$$
$$= (a^{-1})^{p-1} = (a^{-1})^{-n-1} = (a^{-1})^{-(n+1)} = a^{n+1}$$

Suponhamos um dos expoentes positivo (digamos $n \geq 0$) e procedamos por indução sobre ele.

$$n = 0: a^m \cdot a^0 = a^m \cdot 1 = a^m = a^{m+0}$$

Suponhamos $r \geq 0$ e $a^m \cdot a^r = a^{m+r}$

$n = r + 1$:
$a^m \cdot a^{r+1} = a^m \cdot (a^r \cdot a) = (a^m \cdot a^r) \cdot a = a^{m+r} \cdot a = a^{(m+r)+1} = a^{m+(r+1)}$

Por último, se $m, n < 0$, então $m + n < 0$ e, portanto:

$$a^{m+n} = (a^{-1})^{-(m+n)} = (a^{-1})^{(-m)+(-n)} = (a^{-1})^{-m} \cdot (a^{-1})^{-n} = a^m \cdot a^n$$

Registremos ainda que, por definição, para todo $m \in \mathbb{N}^*$:

$$0^m = 0$$

Propomos como exercício a demonstração das seguintes propriedades:

- $(a^m)^n = a^{mn}$, $\forall a \in \mathbb{Q}^*$ e $\forall m, n \in \mathbb{Z}$
- $(a^n)^{-1} = (a^{-1})^n = a^{-n}$, $\forall a \in \mathbb{Q}^*$ e $\forall n \in \mathbb{Z}$.

3.4 Relação de ordem em $\mathbb{Q}$

Seja $a = \dfrac{m}{n} \in \mathbb{Q}$. Como

$$a = \frac{m}{n} = \frac{-m}{-n}$$

pois $m(-n) = n(-m)$, então sempre podemos considerar, para todo $a \in \mathbb{Q}$, uma representação em que o denominador seja maior que zero (em $\mathbb{Z}$).

Por exemplo:

$$\frac{2}{-3} = \frac{-2}{3} \text{ e } \frac{-2}{-3} = \frac{2}{3}$$

DEFINIÇÃO 5 Sejam a e b elementos de $\mathbb{Q}$ e tomemos, para cada um deles, uma representação $a = \frac{m}{n}$ e $b = \frac{r}{s}$ em que o denominador seja estritamente positivo. Nessas condições, diz-se que a *é menor que ou igual a* b, e escreve-se $a \leqslant b$, se $ms \leqslant nr$ (obviamente esta última relação é considerada em $\mathbb{Z}$). Equivalentemente pode-se dizer que b *é maior que ou igual a* a e anotar $b \geqslant a$. Com as mesmas hipóteses, se $ms < nr$, diz-se que a *é menor que* b (notação: $a < b$) ou que b *é maior que a* (notação: $b > a$).

Por exemplo:

$$\frac{-2}{3} < \frac{1}{4} \text{ porque } -8 < 3$$

$$\frac{5}{6} > \frac{4}{5} \text{ porque } 25 > 24$$

Pode-se mostrar que a definição 5 não depende dos pares ordenados eventualmente escolhidos para expressar a e b.

Um elemento $a = \frac{m}{n} \in \mathbb{Q}$ onde $n > 0$, se diz *positivo* se $a \geqslant 0$. Lembrando que $0 = \frac{0}{1}$, então:

$$a \geqslant 0 \iff \frac{m}{n} \geqslant \frac{0}{1} \iff m \geqslant 0$$

Quando $a > 0$, o que equivale (supondo como sempre $n > 0$) a $m > 0$, a se diz *estritamente positivo*. Se $a \leqslant 0$ ($\iff m \leqslant 0$ se $n > 0$), diz-se que a é *negativo* e se $a < 0$ ($\iff m < 0$ se $n > 0$), então o elemento a é chamado *estritamente negativo*.

Exemplo 2: Sejam $a, b \in \mathbb{Q}$. Mostremos que se $a > b$, então existe $h \in \mathbb{Q}$, $h > 0$, de maneira que $a = b + h$.

De fato, suponhamos $a = \frac{r}{s}$ e $b = \frac{t}{s}$, onde $s > 0$. Como

$$\frac{r}{s} > \frac{t}{s}$$

então $r > t$ (em $\mathbb{Z}$) e, portanto, existe $n \in \mathbb{Z}$, $n > 0$, de modo que $r = t + n$.

Daí

$$\frac{r}{s} = \frac{t+n}{s} = \frac{t}{s} + \frac{n}{s}$$

onde

$$h = \frac{n}{s} > 0$$

pois $n > 0$.

Mostraremos a seguir que $\leqslant$, conforme definição 5, é uma relação de ordem total sobre $\mathbb{Q}$, compatível com a adição e a multiplicação definidas em 3.1 e 3.2. Para tanto admitiremos que todos os denominadores que intervierem nos enunciados das propriedades sejam inteiros estritamente positivos.

$\mathbf{O_1}$ $\frac{m}{n} \leqslant \frac{m}{n}$ (reflexiva)

Evidente, pois $mn \leqslant nm$

$\mathbf{O_2}$ $\frac{m}{n} \leqslant \frac{r}{s}$ e $\frac{r}{s} \leqslant \frac{m}{n} \Rightarrow \frac{m}{n} = \frac{r}{s}$ (anti-simétrica)

Como $ms \leqslant nr$ e $rn \leqslant sm$ (em $\mathbb{Z}$), então $ms = nr$. Logo:

$$\frac{m}{n} = \frac{r}{s}$$

$\mathbf{O_3}$ $\frac{m}{n} \leqslant \frac{r}{s}$ e $\frac{r}{s} \leqslant \frac{p}{q} \Rightarrow \frac{m}{n} \leqslant \frac{p}{q}$ (transitiva)

De fato, como $ms \leqslant nr$ e $rq \leqslant sp$, multiplicando a primeira dessas relações por $q > 0$ e a segunda por $n > 0$:

$$msq \leqslant nrq \text{ e } rqn \leqslant spn$$

Daí, usando a transitividade de $\leqslant$ em $\mathbb{Z}$,

$$msq \leqslant spn$$

E, uma vez que $s > 0$, pode-se concluir que

$$mq \leqslant pn$$

Logo:

$$\frac{m}{n} \leqslant \frac{p}{q}$$

$\mathbf{O_4}$ $\frac{m}{n} \leqslant \frac{r}{s}$ ou $\frac{r}{s} \leqslant \frac{m}{n}$

Evidente, pois em $\mathbb{Z}$: $ms \leqslant nr$ ou $nr \leqslant ms$.

Nota: As propriedades $\mathbf{O_1}$ a $\mathbf{O_4}$ garantem que $\leqslant$, conforme definição 5, é uma relação de ordem total sobre $\mathbb{Q}$.

O_5 $\frac{m}{n} \leqslant \frac{r}{s} \Rightarrow \frac{m}{n} + \frac{p}{q} \leqslant \frac{r}{s} + \frac{p}{q}$, para todo $\frac{p}{q} \in \mathbb{Q}$ ($\leqslant$ é compatível com a adição de $\mathbb{Q}$).

De fato, como por hipótese $ms \leqslant nr$, então $msq^2 \leqslant nrq^2$, e daí:

$$msq^2 + pnsq \leqslant nrq^2 + pnsq$$

Ou seja:

$$(mq + pn)sq \leqslant nq(rq + ps)$$

Donde:

$$\frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq} \leqslant \frac{rq + ps}{sq} = \frac{r}{s} + \frac{p}{q}$$

O_6 $\frac{m}{n} \leqslant \frac{r}{s}$ e $0 \leqslant \frac{p}{q} \Rightarrow \frac{m}{n} \cdot \frac{p}{q} \leqslant \frac{r}{s} \cdot \frac{p}{q}$ ($\leqslant$ é compatível com a multiplicação de $\mathbb{Q}$).

Por hipótese, $ms \leqslant nr$ e $p \geqslant 0$ (além de $n, s, q > 0$). Assim $pq \geqslant 0$ e portanto

$$(ms)(pq) \leqslant (nr)(pq)$$

ou

$$(mp)(sq) \leqslant (nq)(rp)$$

onde $sq > 0$ e $nq > 0$. Logo:

$$\frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq} \leqslant \frac{rp}{sq} = \frac{r}{s} \cdot \frac{p}{q}$$

Nota: Seja K um corpo e suponhamos que sobre K esteja definida uma relação $\leqslant$ tal que: **i** $a \leqslant a$ (reflexiva); **ii** $a \leqslant b$ e $b \leqslant a \Rightarrow a = b$ (anti-simétrica); **iii** $a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$ (transitiva); **iv** $a \leqslant b$ ou $b \leqslant a$, para quaisquer $a, b \in K$; **v** $a \leqslant b \Rightarrow a + c \leqslant b + c$, para todo $c \in K$ ($\leqslant$ é compatível com a adição de $\mathbb{Q}$); **vi** $a \leqslant b$ e $0 \leqslant c \Rightarrow ac \leqslant bc$ ($\leqslant$ é compatível com a multiplicação de $\mathbb{Q}$). Nessas condições diz-se que K é um *corpo ordenado*.

Portanto $\mathbb{Q}$ é um exemplo (evidentemente muito importante) de corpo ordenado. Porém o exemplo mais importante é o dos números reais — a ser focalizado no capítulo V.

Se K é um corpo ordenado e se $a, b \in K$, escreve-se $a < b$ para indicar que $a \leqslant b$ e $a \neq b$. (Esse conceito é coerente com a relação "x é menor que y" conforme definição 5.) Para a relação $<$ num corpo ordenado K, vale a *lei da tricotomia*: "Para quaisquer $x, y \in K$, ou $x = y$ ou $x < y$ ou $y < x$, exclusivamente". De fato a propriedade **iv** impõe que $x \leqslant y$ ou $y \leqslant x$; assim, se $x \neq y$, então $x < y$ ou $y < x$. Não se pode ter simultaneamente $x < y$ e $y < x$ pois isto equivale a ($x \leqslant y$ e $x \neq y$) e ($y \leqslant x$ e $y \neq x$), do que segue $x = y$ e $x \neq y$.

Outras propriedades:

As propriedades enunciadas a seguir, envolvendo as relações $\leqslant$, $>$ e $<$ sobre $\mathbb{Q}$, independem todas de m_4, razão pela qual podem ser demonstradas tal como as correspondentes de $\mathbb{Z}$.

Se, a, b, c, d, a_i, b_i indicam elementos genéricos de $\mathbb{Q}$, então:

- $a \leqslant b \iff 0 \leqslant b - a \iff -b \leqslant -a$
- $a < b \iff 0 < b - a \iff -b < -a$
- $a \leqslant b$ e $c \leqslant d \Rightarrow a + c \leqslant b + d$
- $a_i \leqslant b_i (i = 1, 2, \ldots, n) \Rightarrow \sum_{i=1}^{n} a_i \leqslant \sum_{i=1}^{n} b_i$
- Se $a_i \leqslant b_i$ ($i = 1, 2, \ldots, n$) e, para algum r, $1 \leqslant r \leqslant n$, $a_r < b_r$, então
$$\sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i$$
- *Regras de sinais*: **i** $a > 0$ e $b > 0 \Rightarrow ab > 0$; **ii** $a < 0$ e $b < 0 \Rightarrow ab > 0$ **iii** $a < 0$ e $b > 0 \Rightarrow ab < 0$
- $a^2 \geqslant 0$; $a^2 > 0$ sempre que $a \neq 0$
- $a < b$ e $c > 0 \Rightarrow ac < bc$
- $a < b$ e $c < 0 \Rightarrow ac > bc$
- $ac \leqslant bc$ e $c > 0 \Rightarrow a \leqslant b$
- $\sum_{i=1}^{n} a_i^2 \geqslant 0$; $\sum_{i=1}^{n} a_i^2 = 0 \iff a_i = 0$ ($i = 1, 2, \ldots, n$)

PROPOSIÇÃO 1 Para quaisquer $a, b \in \mathbb{Q}$:

i ($a > 0 \Rightarrow a^{-1} > 0$) e ($a < 0 \Rightarrow a^{-1} < 0$)

ii ($0 < a < 1 \Rightarrow 1 < a^{-1}$) e ($1 < a \Rightarrow 0 < a^{-1} < 1$)

iii $0 < a < b \Rightarrow 0 < b^{-1} < a^{-1}$

iv $a < b < 0 \Rightarrow b^{-1} < a^{-1} < 0$

Demonstração:

i Como $a^{-1} \neq 0$, pois $a^{-1} \cdot a = 1$, então $(a^{-1})^2 > 0$. Desta relação e da hipótese $0 < a$ decorre:

$$0 \cdot (a^{-1})^2 < a \cdot (a^{-1})^2$$

Ou seja: $0 < a^{-1}$. Fica como exercício a demonstração da segunda parte.

ii Como $a^{-1} > 0$, em virtude de **i**, então multiplicando os termos de $0 < a < 1$ (hipótese) por a^{-1}:

$$0 \cdot a^{-1} < a \cdot a^{-1} < 1 \cdot a^{-1}$$

o que implica $0 < 1 < a^{-1}$. A demonstração da segunda parte é análoga.

iii Como $a^{-1} > 0$ e $b^{-1} > 0$ em virtude da primeira parte, então $a^{-1} \cdot b^{-1} > 0$. Multiplicando os termos de $0 < a < b$ (hipótese) por $a^{-1} \cdot b^{-1}$:

$$0 \cdot (a^{-1} \cdot b^{-1}) < a \cdot (a^{-1} \cdot b^{-1}) < b \cdot (a^{-1} \cdot b^{-1})$$

Donde: $0 < b^{-1} < a^{-1}$.

iv Fica como exercício. ■

3.5 Imersão de $\mathbb{Z}$ em $\mathbb{Q}$ (os inteiros como particulares números racionais)

Consideremos o número $2 \in \mathbb{Z}$ e o elemento

$$\frac{8}{4} = \{(2, 1); (-2, -1); (4, 2); (-4, -2); \ldots\}$$

por exemplo. É de se esperar, tendo em vista o objetivo da construção de $\mathbb{Q}$, que tais elementos possam ser identificados. Mas o que justificaria essa identificação se se trata de coisas que num primeiro exame se mostram muito diferentes?

Seja $f : \mathbb{Z} \rightarrow \mathbb{Q}$ definida por:

$$f(m) = \frac{m}{1}, \ \forall m \in \mathbb{Z}$$

Para essa aplicação vale o seguinte:

- $f(m) = f(n) \Rightarrow \frac{m}{1} = \frac{n}{1} \Rightarrow m = n$ e, portanto, f é injetora.
- Para quaisquer $m, n \in \mathbb{Z}$:

$$f(m + n) = \frac{m + n}{1} = \frac{m}{1} + \frac{n}{1} = f(m) + f(n)$$

- Para quaisquer $m, n \in \mathbb{Z}$

$$f(mn) = \frac{mn}{1} = \frac{m}{1} \cdot \frac{n}{1} = f(m)\, f(n)$$

- Se $m \leqslant n$, então:

$$f(m) = \frac{m}{1} \leqslant \frac{n}{1} = f(n)$$

Essas propriedades de f significam que a imagem de $\mathbb{Z}$ por f, ou seja

$$\mathrm{Im}(f) = \left\{ \frac{m}{1} \middle| m \in \mathbb{Z} \right\}$$

pode ser vista como uma cópia de $\mathbb{Z}$. Devido a esse fato cada inteiro m se confunde com sua imagem $\frac{m}{1}$ $\left(\text{ou seja, } m = \frac{m}{1}\right)$ e portanto $\mathbb{Z}$ passa a ser identificado com Im(f). Como $\mathrm{Im}(f) \subset \mathbb{Q}$, então $\mathbb{Z} \subset \mathbb{Q}$. Levando em conta que $\mathbb{N} \subset \mathbb{Z}$, pode-se concluir que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. A função f é chamada *função imersão* de $\mathbb{Z}$ em $\mathbb{Q}$.

Isso posto, se $m, n \in \mathbb{Z}$, $n \neq 0$, então:

$$m : n = \frac{m}{1} : \frac{n}{1} = \frac{m}{1} \cdot \frac{1}{n} = \frac{m}{n} \in \mathbb{Q}$$

Por outro lado, dado o número racional $\frac{m}{n}$, então:

$$\frac{m}{n} = \frac{m}{1} \cdot \frac{1}{n} = \frac{m}{1} : \frac{n}{1} = m : n$$

Por isso chamamos cada representação $\frac{m}{n}$ ($m, n \in \mathbb{Z}$; $n \neq 0$) de um número racional dado de *fração ordinária* de numerador m e denominador n. Se mdc (m, n) = 1, a fração se diz *irredutível*.

Ademais, se m é múltiplo de n, digamos $m = nr$ ($r \in \mathbb{Z}$), então:

$$m : n = \frac{m}{n} = \frac{nr}{n} = \frac{r}{1} = r$$

Ou seja, a divisão de um inteiro m por um inteiro $n \neq 0$ não só é sempre possível em $\mathbb{Q}$ como, quando m é múltiplo de n, o resultado coincide com o que se teria em $\mathbb{Z}$.

O conjunto $\mathbb{Q}$, construído da maneira como o fizemos, com a adição, a multiplicação e a relação de ordem que definimos, é o *conjunto dos números racionais* e seus elementos, os *números racionais*, como já havíamos antecipado ao início deste parágrafo.

PROPOSIÇÃO 2 Para quaisquer $a, b \in \mathbb{Q}$, se $a < b$, então existe $c \in \mathbb{Q}$ para o qual vale $a < c < b$.

Demonstração: A hipótese $a, b \in \mathbb{Q}$, $a < b$, implica que $a + a < a + b$ e $a + b < b + b$. Logo $a + a < a + b < b + b$. Mas

$$a + a = 1 \cdot a + 1 \cdot a = (1 + 1)a = 2a$$

e, analogamente, b + b = 2b. Logo:

$$2a < a + b < 2b$$

Multiplicando os termos dessa desigualdade por $\frac{1}{2}$:

$$\frac{1}{2}(2a) < \frac{1}{2}(a + b) < \frac{1}{2}(2b)$$

Como

$$\frac{1}{2}(2a) = \left(\frac{1}{2} \cdot 2\right)a = 1 \cdot a = a$$

e, da mesma forma

$$\frac{1}{2}(2b) = b$$

então:

$$a < \frac{1}{2}(a + b) < b$$

Como

$$c = \frac{1}{2}(a + b) \in \mathbb{Q}$$

o teorema está demonstrado. ■

COROLÁRIO: O conjunto dos elementos estritamente positivos de $\mathbb{Q}$ não tem mínimo.

De fato, se $0 < a$, então

$$0 < \frac{1}{2}a < a$$ ■

Nota: Um corpo K se diz *denso* quando, para quaisquer a, b ∈ K, a < b (o que significa $a \leqslant b$ e $a \neq b$), existe c ∈ K de modo que $0 < c < b$. A proposição 2 mostra exatamente que o corpo ordenado $\mathbb{Q}$ dos números racionais é denso.

PROPOSIÇÃO 3 Se a e b são números racionais e se $b > 0$, então existe $n \in \mathbb{N}^*$ de maneira que $nb > a$.

Demonstração: Podemos supor

$$a = \frac{r}{s} \text{ e } b = \frac{t}{s}$$

onde $s > 0$ e $t > 0$ (pelo fato de $b > 0$). Como já vimos no capítulo III, 6.2, existe $n \in \mathbb{N}^*$ de modo que $nt > r$. Daí segue que $nts > sr$. Logo:

$$\frac{nt}{s} > \frac{r}{s}$$

Mas

$$n\frac{t}{s} = \frac{n}{1}\frac{t}{s} = \frac{nt}{s}$$

Assim:

$$n\frac{t}{s} > \frac{r}{s}$$

Ou seja: $nb > a$.

■

Nota: Um corpo ordenado K se diz *arquimediano* se, para quaisquer a, b ∈ K, b > 0, existe $n \in \mathbb{N}^*$ de maneira que

$$nb = b + b + \dots + b > a \ (\iff a < nb)$$

onde o número de parcelas iguais a b é evidentemente n. Assim, a proposição 3 nos assegura que o corpo ordenado $\mathbb{Q}$ dos números racionais é arquimediano.

EXERCÍCIOS

Nos exercícios deste capítulo usaremos as expressões "números racionais" e "frações ordinárias" com o mesmo significado.

365. Mostre que:

a) $\frac{1\,515}{3\,333} = \frac{15}{33}$ b) $\frac{131\,313}{999\,999} = \frac{13}{99}$ c) $\frac{2\,323}{9\,999} = \frac{23}{99}$

Resolução de a):

$$\frac{1\,515}{3\,333} = \frac{15 \cdot 100 + 15}{33 \cdot 100 + 33} = \frac{15 \cdot (100 + 1)}{33 \cdot (100 + 1)} = \frac{15}{33}$$

366. Ache uma fração ordinária igual a $\frac{1\,001}{715}$ cuja soma do numerador com o denominador seja 48.

367. Ache uma fração ordinária igual a $\frac{399}{1\,463}$ de modo que a diferença entre seu denominador e seu numerador seja 184.

368. Ache duas frações ordinárias de denominadores 5 e 7 cuja soma é igual a $\frac{26}{35}$

369. Ache duas frações ordinárias de denominadores 3 e 11 cuja diferença seja igual a $\frac{6}{33}$.

Resolução: Sejam $\frac{x}{3}$ e $\frac{y}{11}$ as frações procuradas. Então:

$$\frac{x}{3} - \frac{y}{11} = \frac{11x - 3y}{33} = \frac{6}{33}$$

Daí: $11x - 3y = 6$. Uma solução particular dessa equação diofantina é $(-6, -24)$. Logo, uma resposta ao problema é dada pelas frações $\frac{-6}{3} = -2$ e $\frac{-24}{11}$. Como $(-6 - 3t, -24 - 11t)$, $t \in \mathbb{Z}$, é a solução geral da equação diofantina obtida, então todo par de frações

$$\frac{-6 - 3t}{3}, \frac{-24 - 11t}{11} \ (t \in \mathbb{Z})$$

constitui uma solução do exercício.

370. Existem duas frações ordinárias de denominadores 7 e 11, com numeradores positivos, cuja soma seja $\frac{30}{77}$? Justifique a resposta.

371. Sejam $\frac{m}{n}$ e $\frac{r}{s}$ frações ordinárias irredutíveis. Mostre que:

$$\frac{m}{n} = \frac{r}{s} \iff m = \pm r \text{ e } n = \pm s$$

372. Seja $\frac{m}{n}$ uma fração ordinária irredutível. Se $r \in \mathbb{Z}$, prove que

$$r + \frac{m}{n} = \frac{rn + m}{n}$$

também é irredutível.

373. Determine $r \in \mathbb{Z}$ de maneira que as seguintes frações ordinárias representem números inteiros:

a) $\frac{10r}{2r - 1}$ b) $\frac{33r}{3r - 1}$

Sugestão para a): $\frac{10r}{2r - 1} = 5 + \frac{5}{2r - 1}$

374. Se $n \in \mathbb{Z}$, mostre que são irredutíveis as frações:

a) $\frac{n - 1}{n - 2}$ $(n \neq 2)$ b) $\frac{n - 1}{2n - 1}$ c) $\frac{2n + 1}{2n(n + 1)}$ $(n \neq 0, -1)$

375. Se $\frac{m}{n} = \frac{r}{s}$, mostre que

$$\frac{m}{n} = \frac{r}{s} = \frac{mu + rv}{nu + sv}$$

para quaisquer $u, v \in \mathbb{Z}$, ambos não nulos.

376. Sejam $\frac{r}{s}$ e $\frac{m}{n}$ frações irredutíveis. Mostre que

$$\frac{r}{s} + \frac{m}{n} = \frac{rn + ms}{sn}$$

é irredutível se, e somente se, $\text{mdc}(s, n) = 1$.

Resolução:

$\Rightarrow$ Vamos supor $\text{mdc}(s, n) > 1$ e seja p um divisor primo comum a s e a n. Mas então $p \mid (sn)$ e $p \mid (rn + ms)$, o que contraria a hipótese.

$\Leftarrow$ Se a soma não fosse irredutível, então sn e $(rn + ms)$ seriam divisíveis por um conveniente primo p. De $p \mid (sn)$, resulta que $p \mid s$ ou $p \mid n$.

Admitamos que $p|s$, como $p|(rn + ms)$, então $p|(rn)$; como $p \nmid r$ pois mdc $(s, r) = 1$, então $p|n$. Absurdo, já que, por hipótese, mdc $(s, n) = 1$. A hipótese $p|n$ leva igualmente a um absurdo.

377. Sejam r e s inteiros não nulos. Mostre que a fração ordinária $\frac{r^2 + s^2}{rs}$ representa um número inteiro se, e somente se, $r = \pm s$.

378. Mostre que as frações ordinárias $\frac{7n - 1}{4}$ e $\frac{5n + 3}{12}$ não podem representar números inteiros para o mesmo valor de $n \in \mathbb{Z}$.

379. Determine dois inteiros r e s, primos entre si, tais que:

$$\frac{r^2 - s^2}{r^3 - s^3} = \frac{13}{127}$$

Sugestão: Exercício 371.

380. Seja n um inteiro. Mostre que a fração $\frac{n^2 - 1}{3n + 1}$ é irredutível se, e somente se, n é ímpar.

Sugestão: Se $n^2 - 1 = r$ e $3n + 1 = s$, mostre que $s^2 - 2s - 9r = 8$.

381. Determine todas as frações ordinárias $\frac{r}{s}$ tais que $\frac{r - 27}{s} = \frac{r}{s + 12}$.

382. Sejam $\frac{r}{s}$ e $\frac{m}{n}$ frações ordinárias tais que $rn - ms = 1$.

a) Mostre que ambas as frações são irredutíveis.

b) Se $k \in \mathbb{Z}$ e $ks + n \neq 0$, mostre que $\frac{kr + m}{ks + n}$ também é irredutível.

383. Seja $n > 1$ um inteiro. Prove que $\frac{r}{s}$, onde $r = 15n^2 + 8n + 6$ e $s = 30n^2 + 21n + 13$, é irredutível.

Resolução: Notemos que $s = 30n^2 + 21n + 13 = 2(15n^2 + 8n + 6) + (5n + 1) = 2r + (5n + 1)$, ou seja, $s - 2r = 5n + 1$; ademais, $r = 15n^2 + 8n + 6 = (5n + 1)(3n + 1) + 5$. Assim, se $d|r$ e $d|s$, então $d|(s - 2r)$, ou seja $d|(5n + 1)$; mas então $d|5$, visto que $5 = r - (5n + 1)(3n + 1)$, e disso resulta que $d|5n$; donde $d|1$, pois $(5n + 1) - 5n = 1$. Assim $d = \pm 1$ e mdc $(r, s) = 1$.

384. Prove por indução que:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \ldots + \frac{1}{n(n + 1)} = \frac{n}{n + 1} \quad (n \geqslant 1)$$

385. Mostre que as seguintes somas não são números inteiros:

a) $S_1 = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \quad (n > 1)$;

b) $S_2 = \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n + 1} \quad (n > 0)$

Resolução de a): Seja r o maior inteiro positivo tal que $2^r \leqslant n$ e seja k o produto dos ímpares $\leqslant n$. Então o produto $2^{r-1} \cdot k \cdot S_1$ é uma soma de $n - 1$ parcelas, todas números inteiros, exceto $2^{r-1} \cdot k \cdot \frac{1}{2^r} = \frac{k}{2}$. Ora, se S_1 fosse inteiro, o mesmo aconteceria com $\frac{k}{2}$ que é a diferença entre S_1 e a soma de $n - 2$ parcelas inteiras. Como $\frac{k}{2} \notin \mathbb{Z}$, então $S_1 \notin \mathbb{Z}$.

386. J. J. Sylvester (1814-1897) propôs o seguinte método para escrever um número racional a, $0 < a < 1$, como soma de frações unitárias (ver Introdução): **i** achar a maior fração unitária que seja menor que a fração dada; **ii** subtrair essa fração unitária da fração dada; **iii** achar a maior fração unitária menor que a diferença obtida em **ii**; **iv** subtrair desta diferença, a fração unitária obtida em **iii**; **v** continuar o processo até que uma das diferenças seja fração unitária.

Aplique esse processo às seguintes frações: $\frac{13}{20}$, $\frac{4}{15}$, $\frac{9}{24}$ e $\frac{7}{52}$.

Resolução: $\frac{1}{a} < \frac{13}{20} \Rightarrow 20 < 13a$. Logo $a = 2$ é o menor natural para o qual a desigualdade se verifica. $\frac{1}{a} < \frac{13}{20} - \frac{1}{2} = \frac{3}{20} \Rightarrow 20 < 3a$; a escolha neste caso deve ser $a = 7$. Como $\frac{3}{20} - \frac{1}{7} = \frac{1}{140}$ é unitária, então

$$\frac{13}{20} = \frac{1}{2} + \frac{3}{20} = \frac{1}{2} + \frac{1}{7} + \frac{1}{140}$$

387. a) Considere o polinômio unitário $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ $(a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z})$. Se a fração ordinária irredutível $u = \frac{r}{s}$ é raiz de f(x), isto é, f(u) = 0, prove que $s = \pm 1$ e que $r \mid a_0$ (ou seja, u é um divisor inteiro de a_0).

b) Determine as raízes racionais de $f(x) = x^5 - 2x^4 + 3x^2 + 7x - 9$.

388. Mostre que os seguintes polinômios não admitem raízes racionais:

a) $f(x) = x^2 - 2$ b) $g(x) = x^3 - 2$ c) $h(x) = x^3 + x + 1$

389. Seja K um corpo. Uma aplicação bijetora $f: K \to K$ se diz um *automorfismo* de K se: $f(x + y) = f(x) + f(y)$ e $f(xy) = f(x) f(y)$, para todo par de elementos $x, y \in K$. Mostre, através das etapas seguintes, que o único automorfismo f de $\mathbb{Q}$ é a aplicação idêntica: i $f(1) = 1$; ii $f(-a) = -f(a)$, $\forall a \in \mathbb{Q}$; iii $f(m) = m$, $\forall m \in \mathbb{Z}$; iv $f\left(\frac{1}{n}\right) = \frac{1}{n}$, $\forall n \in \mathbb{N}^*$; v $f\left(\frac{m}{n}\right) = \frac{m}{n}$, $\forall m, n \in \mathbb{Z}, n \neq 0$.

Resolução: ii Como $f(0) = f(0 + 0) = f(0) + f(0)$, então, pela lei do cancelamento da adição, $f(0) = 0$. Assim, $\forall a \in \mathbb{Q}$: $f(-a) + f(a) = f((-a) + a) = f(0) = 0$; então $f(-a) = -f(a)$. iv $1 = f(1) = f\left(\frac{n}{n}\right) = f\left(n \cdot \frac{1}{n}\right) = f\left(\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}\right) = f\left(\frac{1}{n}\right) + f\left(\frac{1}{n}\right) + \ldots + f\left(\frac{1}{n}\right) = nf\left(\frac{1}{n}\right) \Rightarrow f\left(\frac{1}{n}\right) = \frac{1}{n}$. v Admitindo $n > 0$, o que sempre é possível, $f\left(\frac{m}{n}\right) = f\left(m \cdot \frac{1}{n}\right) = f(m) f\left(\frac{1}{n}\right) = m \frac{1}{n} = \frac{m}{n}$.

390. a) Ache duas frações ordinárias positivas, respectivamente iguais a $\frac{1}{2}$ e $\frac{4}{5}$ de maneira que a soma de seus termos (numerador e denominador) coincida e seja a menor possível.

b) Idem para as frações $\frac{2}{3}$, $\frac{1}{5}$ e $\frac{2}{7}$.

Resolução de a): As frações procuradas são do tipo $\frac{x}{2x}$ e $\frac{4y}{5y}$, onde $x, y \in \mathbb{Z}_+^*$. Devemos impor que $x + 2x = 4y + 5y = s$, de onde resulta $x = \frac{s}{3}$ e $y = \frac{s}{9}$. Como s deve ser a menor possível, então s = mmc (3,9) = 27 (pois x e y são inteiros). Daí x = 9 e y = 3. A resposta é, então: $\frac{9}{18}$ e $\frac{12}{15}$.

391. Seja $\frac{r}{s}$ um número racional positivo não nulo. Prove que:

$$\frac{r}{s} + \frac{s}{r} \geqslant 2$$

Em que condições ocorre a igualdade?

392. a) Seja a um número racional tal que $0 < a < 1$. Mostre que existe $r \in \mathbb{N}^*$ para o qual

$$\frac{1}{r+1} \leqslant a < \frac{1}{r}$$

b) Ache r, conforme parte a), nos seguintes casos: $a = \frac{7}{22}$ e $a = \frac{47}{60}$.

393. Se $n > 1$ é um inteiro, prove que:

$$\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n} > \frac{1}{2}$$

394. Sejam $a = \frac{m}{n}$ e $b = \frac{r}{s}$ números racionais, $a < b$. Se $p, q \in \mathbb{N}^*$, prove que:

$$a < \frac{mp + rq}{np + sq} < b$$

4. Valor absoluto (ou Módulo)

DEFINIÇÃO 6 Damos o nome de *valor absoluto* de um elemento $a \in \mathbb{Q}$ ao próprio a se $a \geqslant 0$ e ao oposto de a, se $a < 0$. O valor absoluto de a é indicado por $|a|$. Assim:

$$|a| = a, \text{ se } a \geqslant 0 \text{ e } |a| = -a, \text{ se } a < 0$$

Obviamente, então, $|a| \geqslant 0$ para todo $a \in \mathbb{Q}$. **Por exemplo:**

$$\left|-\frac{1}{2}\right| = -\left(-\frac{1}{2}\right) = \frac{1}{2} \text{ e } \left|\frac{2}{3}\right| = \frac{2}{3}$$

PROPOSIÇÃO 4 Para quaisquer $a, b \in \mathbb{Q}$ valem as seguintes relações:

i $-|a| \leqslant a \leqslant |a|$

ii $|a+b| \leqslant |a| + |b|$

iii $|a| - |b| \leqslant |a-b| \leqslant |a+b|$

iv $|ab| = |a||b|$

v Se $b \neq 0$, então $|b^{-1}| = |b|^{-1}$ e $|ab^{-1}| = |a||b|^{-1}$

Demonstração: As propriedades de **i** a **iv** podem ser provadas da mesma maneira que suas similares em $\mathbb{Z}$ (cap. III, 5), Quanto a **v**, observemos que:

$$bb^{-1} = 1 \Rightarrow |bb^{-1}| = |b||b^{-1}| = |1| = 1$$

de onde decorre que $|b^{-1}|$ é o inverso de $|b|$ e portanto $|b^{-1}| = |b|^{-1}$. Por último

$$|ab^{-1}| = |a||b^{-1}| = |a||b|^{-1}$$ ■

5. A função maior inteiro (sobre $\mathbb{Q}$)

DEFINIÇÃO 7 Seja a um número racional. Denotamos por $[a]$ o maior inteiro que não ultrapassa a. Ou seja:

$$[a] = \max\{m \in \mathbb{Z} \mid m \leqslant a\}$$

A função de $\mathbb{Q}$ em $\mathbb{Z}$ definida por $x \rightarrow [x]$ chama-se *função maior inteiro* (sobre $\mathbb{Q}$).

Por exemplo:

$$[5] = 5; \left[\frac{5}{2}\right] = 2; \left[-\frac{5}{2}\right] = -3$$

PROPOSIÇÃO 5 Se a e b são números racionais quaisquer, então:

i $[a] \leqslant a < [a] + 1$ (logo $0 \leqslant a - [a] < 1$)

ii $a \leqslant b \Rightarrow [a] \leqslant [b]$ (a função maior inteiro é crescente)

iii $[a+m] = [a] + m$, para todo $m \in \mathbb{Z}$

iv $[a] + [b] \leqslant [a+b] \leqslant [a] + [b] + 1$

Demonstração:

i É uma decorrência imediata da definição 7.

ii Suponhamos $[b] < [a]$, para um certo par $a, b \in \mathbb{Q}$, $a \leqslant b$. Sendo $[b]$ e $[a]$ inteiros, então $[b] + 1 \leqslant [a]$. Mas $b < [b] + 1$ (devido a i) e portanto $b < [a]$. Como $[a] \leqslant a$, então $b < a$, o que é absurdo.

iii Se $a_1 = a - [a]$, então $0 \leqslant a_1 < 1$ e $a = [a] + a_1$. Daí

$$[a+m] = [[a] + m + a_1] = [a] + m$$

uma vez que $[a] + m \in \mathbb{Z}$.

iv Façamos $a_1 = a - [a]$, $b_1 = b - [b]$ e $d = a + b - [a+b]$. Então $0 \leqslant a_1, b_1, d < 1$, $a = [a] + a_1$, $b = [b] + b_1$ e $a + b = [a+b] + d$. Daí:

$$a + b = [a] + [b] + (a_1 + b_1), \; 0 \leqslant a_1 + b_1 < 2$$

Como $[a] + [b] \in \mathbb{Z}$ pode-se aplicar **iii** à última igualdade, obtendo-se

$$[a+b] = [a] + [b] + [a_1 + b_1]$$

e como $[a_1 + b_1] = 0$ ou $[a_1 + b_1] = 1$, então:

$$[a+b] \leqslant [a] + [b] + 1 \qquad (*)$$

Por outro lado, levando em conta que $0 \leqslant a_1 + b_1 \leqslant 2$, então $[a_1 + b_1] \geqslant 0$. Donde

$$[a] + [b] \leqslant [a] + [b] + [a_1 + b_1] = [a+b] \qquad (**)$$

As conclusões (*) e (**) garantem a validade de **iv**. ■

PROPOSIÇÃO 6 Sejam m e n inteiros, $n > 0$. Se q é o quociente da divisão euclidiana de m por n, então $q = \left[\frac{m}{n}\right]$.

Demonstração: Vamos supor $m = nq + r$ $(0 \leqslant r < n)$. Então

$$\frac{m}{n} = \frac{nq + r}{n} = \frac{nq}{n} + \frac{r}{n} = q + \frac{r}{n}$$

Como $0 \leqslant r < n$, então

$$0 = \frac{0}{1} \leqslant \frac{r}{n} < \frac{1}{1} = 1$$

e portanto:

$$\left[\frac{r}{n}\right] = 0$$

Levando em conta **iii** da proposição anterior:

$$\left[\frac{m}{n}\right] = \left[q + \frac{r}{n}\right] = q + \left[\frac{r}{n}\right] = q \qquad ■$$

Exemplo 3: Mostremos que o expoente com que um número primo $p > 0$ aparece como fator de $n!$, para todo $n \geqslant 1$, é:

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots$$

É claro que se $p > n$, então p não é fator primo de n (logo de nenhum dos fatores de $n!$) e portanto se pode dizer que o expoente de p em $n!$ é zero. Como, neste caso, $n < p^r$ $(r \geqslant 1)$, então também

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots = 0$$

Se $p \leqslant n$, como o quociente da divisão de n por p é $\left[\frac{n}{p}\right]$ (proposição 6), então p é divisor dos seguintes fatores de $n!$: $p, 2p, \dots, \left[\frac{n}{p}\right]p$ (e apenas destes), visto que $\left[\frac{n}{p}\right]$ p é o último múltiplo de p que não supera n. Assim, p é divisor de $\left[\frac{n}{p}\right]$ fatores de $n!$. Uma argumentação análoga mostra que, desses $\left[\frac{n}{p}\right]$ fatores, aqueles que são múltiplos de p^2 totalizam $\left[\frac{n}{p^2}\right]$. E assim por diante. Logo, o expoente de p em $n!$ é, efetivamente, a soma dada no enunciado.

Por exemplo, o expoente de 3 em 20! é

$$\left[\frac{20}{3}\right] + \left[\frac{20}{9}\right] = 6 + 2 = 8$$

6. Números racionais decimais

DEFINIÇÃO 8 Todo número racional que puder ser escrito sob a forma

$$\frac{r}{10^n}$$

onde $r \in \mathbb{Z}$ e $n \in \mathbb{N}$, chama-se *número racional decimal*.

Por exemplo:

$$\frac{3}{10}, \frac{-19}{100}, \frac{1}{250} = \frac{4}{1\,000}$$

PROPOSIÇÃO 7 Um elemento $a \in \mathbb{Q}$ é um número racional decimal se, e somente se, existem $r \in \mathbb{Z}$ e $\alpha, \beta \in \mathbb{N}$, de maneira que

$$a = \frac{r}{2^\alpha \cdot 5^\beta}$$

Demonstração:

$\Leftarrow$ Vamos supor a conforme o enunciado. Então, admitindo-se por exemplo $\alpha \geqslant \beta$:

$$a = \frac{r}{2^\alpha \cdot 5^\beta} = \frac{r \cdot 5^{\alpha-\beta}}{2^\alpha \cdot 5^\beta \cdot 5^{\alpha-\beta}} = \frac{5^{\alpha-\beta} \cdot r}{10^\alpha}$$

e portanto a é um número racional decimal

$\Rightarrow$ Se a é racional decimal, então existem $r \in \mathbb{Z}$ e $n \in \mathbb{N}^*$ de modo que

$$a = \frac{r}{10^n} = \frac{r}{2^n \cdot 5^n}$$

o que encerra a demonstração. ■

6.1 A representação decimal

Consideremos, a título de ilustração para as considerações que faremos neste item, o seguinte número racional decimal:

$$\frac{12\,345}{1\,000}$$

Mais um detalhe: se a é inteiro (e todo inteiro é um racional decimal), então a representação decimal de a é o próprio a. De fato, neste caso podemos supor $r = 0$ e então $a_1 = a_2 = \ldots = a_r = 0$.

Apesar da grande vantagem prática da representação decimal sobre a fracionária, sua adoção foi um processo historicamente demorado. Um dos motivos dessa demora foi, com certeza, a dificuldade de estender essa representação adequadamente aos números racionais não decimais. Este assunto será focalizado no capítulo V (8).

Exemplo 4: O papel desempenhado pelos números racionais decimais em nosso sistema de numeração é ocupado, num sistema posicional qualquer de base $b > 1$, pelas frações:

$$a = \frac{n}{b^r} \quad (n, r \geqslant 0)$$

Consideremos por exemplo $b = 2$. Se a representação binária de n é

$$n = (b_1 b_2 \ldots b_s a_1 a_2 \ldots a_r)_2 =$$
$$a_r + a_{r-1} \cdot 2 + \ldots + a_1 \cdot 2^{r-1} + b_s \cdot 2^r + \ldots + b_1 \cdot 2^{r+s-1}$$

então

$$a = \frac{n}{2^r} = \frac{2^r \cdot m + a_1 \cdot 2^{r-1} + \ldots + a_{r-1} \cdot 2 + a_r}{2^r} =$$

$$= m + \frac{a_1}{2} + \frac{a_2}{2^2} + \ldots + \frac{a_r}{2^r}$$

onde

$$m = b_s + b_{s-1} \cdot 2 + \ldots + b_1 \cdot 2^{s-1} = (b_1 b_2 \ldots b_s)_2$$

além de, obviamente, $0 \leqslant a_i, b_j < 2$. A *representação binária* de a é:

$$a = (m, a_1 a_2 \ldots a_r)_2$$

Por exemplo, se $n = 27$, então $n = (11\,011)_2$. Se considerarmos

$$a = \frac{n}{2^3}$$

então $r = 3$ e portanto $a_3 = 1$, $a_2 = 1$, $a_1 = 0$, $b_2 = 1$ e $b_1 = 1$. Donde

$$a = (m, 011)_2$$

onde $m = (11)_2 = 3$.

EXERCÍCIOS

395. Determine:

a) $\left[\frac{3\,077}{1\,538}\right]$

b) $\left[-\frac{3\,075}{1\,538}\right]$

c) $\left[m - \frac{1}{2}\right]$ onde $m \in \mathbb{Z}$ $(m < 0)$

d) $\frac{m+1}{m}$, $m \neq 0$

396. Mostre que $[a] + [-a] = 0$ ou -1, conforme a seja inteiro ou não.

Sugestão: Se $a - [a] = a_1$, então $0 \leqslant a_1 < 1$ e $-a = -[a] - 1 + (1 - a_1)$.

397. Se a e b são números racionais positivos, mostre que $[a][b] \leqslant [ab]$.

398. Mostre que:

$$\left[\frac{a}{n}\right] = \left[\frac{[a]}{n}\right]$$

para todo inteiro $n > 0$.

Resolução: Seja $k = \left[\frac{a}{n}\right] - \left[\frac{a}{n}\right]$. Então $a = n\left[\frac{a}{n}\right] + kn$, onde $0 \leqslant kn < n$ (pois $0 \leqslant k < 1$ e $n > 0$). Logo (proposição 5, **iii**): $[a] = n\left[\frac{a}{n}\right] + [kn]$, o que implica $\frac{[a]}{n} = \left[\frac{a}{n}\right] + \frac{[kn]}{n}$. Usando mais uma vez a parte **iii** da proposição citada, considerando que $0 \leqslant \frac{[kn]}{n} < 1$:

$$\left[\frac{[a]}{n}\right] = \left[\frac{a}{n}\right]$$

399. Mostre que: $[a] + [b] + [a+b] \leqslant [2a] + [2b]$

Sugestão: Considere $a = [a] + a_1$, $0 \leqslant a_1 < 1$, e $b = [b] + b_1$, $0 \leqslant b_1 < 1$. Examine os casos em que nenhum, um ou ambos os números a_1 e b_1 são maiores ou iguais a $\frac{1}{2}$.

400. Sejam a e b $\in \mathbb{N}$, ambos maiores que 1. Prove que:

$$\left[\frac{a}{b}\right] + \left[\frac{a}{b} + \frac{1}{b}\right] + \ldots + \left[\frac{a}{b} + \frac{b-1}{b}\right] = a$$

Resolução (para o caso $1 < a < b$): Na seqüência de numeradores a, $a + 1, \ldots, a + b - 1$ aparece b pois $a < b$ e $b < a + b - 1$ (já que $1 < a$). Do colchete correspondente ao numerador b em diante, todos são iguais a 1. Por exemplo, o primeiro deles é $\left[\frac{a}{b} + \frac{b-a}{b}\right] = \left[\frac{b}{b}\right] = 1$ e o último $\left[\frac{a}{b} + \frac{b-1}{b}\right] = \left[\frac{b}{b} + \frac{a-1}{b}\right] = 1$, pois $a - 1 < b$. Como o número destes colchetes iguais a 1 é a, e todos os anteriores são nulos, então a soma efetivamente é igual a a.

401. Mostre que 1 000! termina em 249 zeros.

Sugestão: Exemplo 3.

402. Determine quais dos seguintes números são racionais decimais e ponha cada um destes na representação decimal.

a) $\frac{1}{256}$ b) $\frac{7}{2\,880}$ c) $\frac{1}{4\,375}$ d) $\frac{-13}{1\,040}$

403. Determine as frações ordinárias cuja representação decimal é a seguinte:

a) 12,0178 c) 0,01075
b) −6,0001 d) −0,14005

404. a) Ache o menor número decimal positivo pelo qual se devem multiplicar as frações $\frac{5}{16}$ e $\frac{5}{8}$ a fim de obter produtos inteiros.

b) Ache o menor número decimal positivo que, dividido pelas frações $\frac{16}{75}$ e $\frac{4}{15}$, fornece quocientes inteiros.

Resolução de a): Se $a = \frac{r}{10^n}$ é o número procurado, então

$$\frac{r}{10^n} \cdot \frac{5}{16} = \frac{r}{2^{n+4} \cdot 5^{n-1}} \quad \text{e} \quad \frac{r}{10^n} \cdot \frac{5}{8} = \frac{r}{2^{n+3} \cdot 5^{n-1}}$$

devem ser inteiros. O menor valor de r para que isso aconteça é $\text{mmc}(2^{n+4} \cdot 5^{n-1}, 2^{n+3} \cdot 5^{n-1}) = 2^{n+4} \cdot 5^{n-1}$. Assim

$$a = \frac{2^{n+4} \cdot 5^{n-1}}{10^n} = \frac{2^4}{5} = 3{,}2$$

405. Escreva em ordem crescente os seguintes números decimais:

a = 0,245132 c = 0,245232
b = 0,245213 d = 0,245123.

406. Sejam $x = 0,\ a_1a_2 \ldots a_ra_{r+1}a_{r+2} \ldots a_t$ e $y = 0,\ a_1a_2 \ldots a_rb_{r+1}b_{r+2} \ldots b_t$ números racionais decimais. Se $a_{r+1} > b_{r+1}$, prove que $x > y$.

407. a) Mostre que $\frac{2n+1}{n(n+1)}$ é irredutível, para todo $n \in \mathbf{Z}$, $n \neq 0$, $n \neq -1$.

b) Determine n a fim de que essa fração represente um número racional decimal.

Resolução de b): Devemos impor que $n(n+1) = 2^\alpha \cdot 5^\beta$ $(\alpha, \beta \geq 0)$. Como mdc $(n, n+1) = 1$, então há duas possibilidades: ($n = 2^\alpha$ e $n + 1 = 5^\beta$) ou ($n = 5^\beta$ e $n + 1 = 2^\alpha$). Examinemos a primeira. De $5^\beta = 2^\alpha + 1$ segue que $2^\alpha = 5^\beta - 1 = (5 - 1)(5^{\beta-1} + \ldots + 5 + 1) = 4 \cdot (5^{\beta-1} + \ldots + 5 + 1)$. É claro que $\alpha = 2$ e $\beta = 1$ fornecem uma solução para o problema: neste caso $n = 4$. Vamos supor que pudesse haver uma solução para $\alpha > 2$. Então $2^{\alpha-2} = 1 + 5 + \ldots + 5^{\beta-1}$, o que obriga β a ser par; daí

$$\begin{aligned} &1 + 5 + 5^2 + \ldots + 5^{\beta-2} + 5^{\beta-1} = \\ &= (1 + 5) + 5^2(1 + 5) + \ldots + 5^{\beta-2}(1 + 5) \end{aligned}$$

e como 3 divide esta soma, teria também que dividir $2^{\alpha-2}$, o que não é possível. Donde $n = 4$ é a única solução.

408. Dê a representação binária e a representação 6-nária (base 6) da fração $\frac{15}{2^4}$.

409. Se $(3{,}41)_8$ é a representação na base 8 de um certo número racional, determine sua representação decimal e sua representação binária.

410. Qual dos seguintes números racionais é o maior?

$$a = 4 + \frac{5}{7} + \frac{3}{7^2} + \frac{6}{7^3} + \frac{6}{7^4}$$

$$b = 4 + \frac{5}{7} + \frac{4}{7^2} + \frac{1}{7^3} + \frac{1}{7^4}$$

411. Ache $x, y \in \mathbb{N}^*$ de maneira que $\frac{x}{2} - \frac{y}{5} = 0{,}3$ e a soma $x + y$ seja a maior possível. E para que $x + y$ seja a menor possível, como devem ser $x, y \in \mathbb{N}^*$?

412. O sistema de numeração babilônico de base 60 deixou vestígios que se traduzem na medida de ângulos e do tempo. Isso posto:

a) Passe 7h 15 min 9 seg para o sistema decimal.
b) Passe 17° 12' 18'' para o sistema decimal.
c) Se um "relógio decimal" marca 12,15 horas, expresse essa marcação em horas, minutos e segundos.

Resolução de b):

$17°\,12'\,18'' = 17 + \frac{12}{60} + \frac{18}{3\,600} = 17 + \frac{1}{5} + \frac{1}{200}$. Como

$$\frac{1}{5} + \frac{1}{200} = \frac{41}{200} = 0{,}205$$

então a resposta é 17,205 graus.

413. Justifique as seguintes regras:

a) $(m, a_1a_2 \ldots a_r) \cdot (0{,}00 \ldots 01) = 0{,}00 \ldots 0\, m\, a_1a_2 \ldots a_r$, onde o número de zeros no segundo membro é igual ao número de zeros do segundo fator do primeiro membro.
b) Se $s > r$, então $10^r \cdot (m, a_1\, a_2 \ldots a_s) = m a_1\, a_2 \ldots a_r,\, a_{r+1}\, a_{r+2} \ldots a_s$.
c) Se $s = r$, então $10^r \cdot (m, a_1\, a_2 \ldots a_s) = m a_1\, a_2 \ldots a_s$.
d) Se $s < r$, então $10^r \cdot (m, a_1\, a_2 \ldots a_s) = m a_1\, a_2 \ldots a_s\, 0 \ldots 0$, onde o número de zeros é $r - s$.

414. Os três problemas a seguir envolvem a idéia de porcentagem. Lembremos que 1% = 0,01.

a) (Fuvest-88) Aumentando-se os lados a e b de um retângulo de 15% e 20%, respectivamente, a área do retângulo é aumentada de:

i) 35%   iii) 3,5%   v) 38%
ii) 30%   iv) 3,8%

b) (Fuvest-84) Em uma prova de 25 questões, cada resposta certa vale 0,4 e cada resposta errada −0,1. Um aluno resolveu todas as questões e teve nota 0,5. Qual a porcentagem de acertos desse aluno?

i) 25%   iii) 20%   v) 5%
ii) 24%   iv) 16%

c) Numa prova de fundo um corredor percorre os primeiros 60% do percurso à velocidade de 20 km/h e o restante a 18 km/h. Se o tempo total gasto por ele foi de duas horas, qual o comprimento do percurso?

CAPÍTULO V

OS NÚMEROS REAIS

1. Medida de um segmento de reta: primeira abordagem

Consideremos dois segmentos de reta AB e CD. Suponhamos que em CD seja possível determinar n pontos ($n \geqslant 1$) $A_1, A_2, \ldots, A_n$, onde $A_n = D$, de maneira que $CA_1, A_1A_2, \ldots, A_{n-1}A_n = A_{n-1}D$ sejam todos congruentes a AB. Dizemos então que CD é *múltiplo* de AB ou que AB é *submúltiplo* de CD e escrevemos:

$$CD = n \cdot AB$$

ou

$$AB = \frac{1}{n} \cdot CD$$

(Figura 1)

A B

C A_1 A_2 A_{n-1} $D = A_n$

Em particular, um segmento de reta é sempre múltiplo (e também submúltiplo) dele mesmo. Neste caso n = 1.

Por definição $0 \cdot AB$ é o segmento de reta nulo, para quaisquer pontos A e B.

O conceito de *soma* de segmentos permite concluir que

$$r \cdot AB + s \cdot AB = (r + s) \cdot AB$$

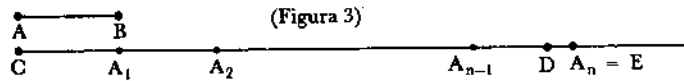
para quaisquer $r, s \in \mathbb{N}$ e para todo segmento de reta AB (figura 2).

(Figura 2)

Nesta figura CD + DE = CE, onde $CD = 5 \cdot AB$, $DE = 3 \cdot AB$ e $CE = 8 \cdot AB$

Lembremos o *axioma de Arquimedes* da geometria euclidiana. Dados os segmentos de reta AB e CD, existe $n \in \mathbb{N}^*$ de maneira que

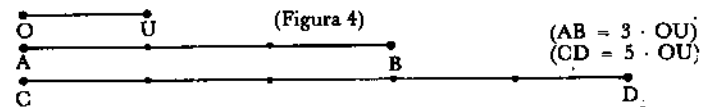
$$n \cdot AB > CD \; \left(\Longleftrightarrow \frac{1}{n} \cdot CD < AB \right)$$

Isso significa que é possível determinar sobre a reta CD um ponto E tal que D está entre C e E e $CE = n \cdot AB$ (figura 3).

(Figura 3)

Dois segmentos de reta AB e CD se dizem *comensuráveis* se é possível encontrar um segmento de reta não nulo OU de maneira que

$$AB = m \cdot OU$$
$$CD = n \cdot OU$$

para convenientes $m, n \in \mathbb{N}$. Ou seja, ambos devem ser múltiplos de um mesmo segmento OU. Na figura 4, AB e CD são comensuráveis.

(Figura 4) $(AB = 3 \cdot OU)$ $(CD = 5 \cdot OU)$

Começaremos a focalizar agora a noção de medida de um segmento de reta AB. Para tanto é preciso antes fixar um segmento de reta u, tomado como *unidade de comprimento*. A idéia é procurar saber "quantas vezes" AB "contém" u.

Vejamos inicialmente como isso se faz quando AB e u são comensuráveis. Neste caso (fig. 5):

$$u = r \cdot OU$$
$$AB = s \cdot OU$$

para algum OU e para convenientes $r, s \in \mathbb{N}$. Então

$$OU = \frac{1}{r} \cdot u$$

e portanto

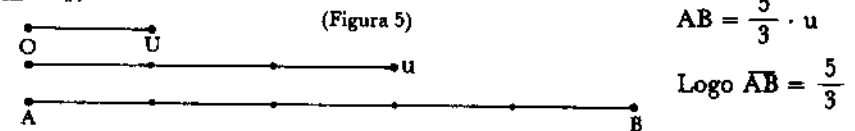
$$AB = s \cdot \left(\frac{1}{r} \cdot u \right)$$

o que representamos por:

$$AB = \frac{s}{r} \quad u$$

Por isso se diz neste caso que a medida de AB é $\frac{s}{r}$ e escreve-se

$$\overline{AB} = \frac{s}{r}$$

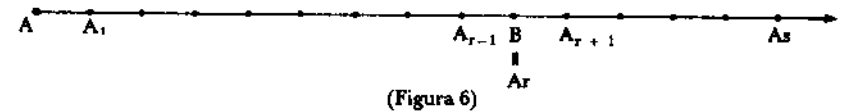
(lê-se: medida de AB igual a $\frac{s}{r}$). Naturalmente, na última igualdade está subentendida a unidade de comprimento. Observe-se que se $u = AB$, então $\overline{AB} = 1$.

(Figura 5)

$$AB = \frac{5}{3} \cdot u$$

$$\text{Logo } \overline{AB} = \frac{5}{3}$$

Outra observação que convém fazer é que, dado um segmento de reta u e dados $r, s \in \mathbb{N}^*$, sempre há segmentos de reta cuja medida (tomando u como unidade de comprimento) é $\frac{s}{r}$.

Examinaremos apenas o caso $s > r$. Façamos $u = AB$ (figura 6) e tomemos $A_1, A_2, \ldots, A_r, A_{r+1}, \ldots, A_s$ na semi-reta $\overrightarrow{AB}$ de maneira que $A_r = B$ e $AA_1, A_1A_2, \ldots, A_{r-1}A_r, A_rA_{r+1}, \ldots, A_{s-1}A_s$ sejam congruentes entre si — o que sempre é possível no âmbito da geometria euclidiana.

(Figura 6)

Como

$$AA_1 = \frac{1}{r} \cdot AB$$

e

$$AA_s = s \cdot AA_1$$

então

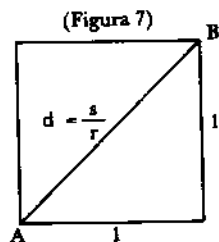
$$AA_s = s \cdot \left(\frac{1}{r} \cdot AB \right) = \frac{s}{r} \cdot AB$$

e considerando que $AB = u$:

$$\overline{AA_s} = \frac{s}{r}$$

Nem sempre porém, escolhida a unidade de comprimento u, o segmento de reta que se quer "medir" e o segmento u são comensuráveis. É o que ocorre quando u é o lado de um quadrado e AB sua diagonal.

De fato, suponhamos, por absurdo, que diagonal e lado fossem comensuráveis (figura 7). Levando em conta as suposições feitas, cada lado tem medida 1 e a diagonal tem medida $\frac{s}{r}$ $(s, r \in \mathbb{N}^*)$. Podemos supor $\mathrm{mdc}(r, s) = 1$.

(Figura 7)

Pelo teorema de Pitágoras

$$\left(\frac{s}{r}\right)^2 = 1^2 + 1^2 = 2$$

e daí:

$$s^2 = 2r^2$$

Logo s é par (pois s^2 é par). Assim $s = 2t$ ($t \in \mathbb{N}^*$) e portanto:

$$4t^2 = 2r^2$$

Daí

$$2t^2 = r^2$$

e então r também é par. Absurdo, já que s e r são primos entre si.

Dois segmentos de reta não comensuráveis se dizem *incomensuráveis*. Coube à escola pitagórica, através do exemplo anterior, o mérito notável da descoberta de segmentos incomensuráveis. Mas isso, ao que parece, não foi motivo de júbilo para seus membros. Como acreditavam que os números naturais e as razões entre eles eram a essência última das coisas, viram com pesar a própria matemática não se ajustar à sua filosofia.

Não demorou muito e o matemático Eudóxio (408?-355? a.C.), também grego, discípulo de Platão, conseguiu elaborar uma teoria das proporções, válida para grandezas em geral, mediante a qual era possível superar com acerto o obstáculo da incomensurabilidade, usando apenas números naturais. Mas essa teoria, apesar de brilhante, era essencialmente geométrica e não levava, como seria desejável, à criação de novos números para expressar a razão entre grandezas incomensuráveis. Pois, como mostra o exemplo da diagonal e do lado de um quadrado, o corpo ordenado $\mathbb{Q}$ não é suficiente para tanto.

Nos parágrafos seguintes construiremos o corpo ordenado dos números reais, uma extensão de $\mathbb{Q}$ onde sempre é possível expressar a razão entre duas grandezas quaisquer de mesma espécie. E em 4.1 daremos a definição de medida no caso de o segmento de reta e a unidade de comprimento serem incomensuráveis.

Até lá falaremos de "aproximações racionais da medida" para este último caso. Vamos supor AB e u incomensuráveis. Para todo $r > 1$, o axioma de

Arquimedes garante que existem múltiplos de $\frac{1}{r} \cdot u$ que superam AB. Se $\frac{s+1}{r} \cdot u$ é o menor deles, então:

$$\frac{s}{r} \cdot u < AB < \frac{s+1}{r} \cdot u$$

$AM = \frac{11}{3} \cdot u$

$AN = \frac{12}{3} \cdot u$

u

A M B N

(Figura 8)

Isso significa que em AB há um ponto interno M tal que $AM = \frac{s}{r} \cdot u$ e que na semi-reta $\overrightarrow{AB}$ há um ponto N, à direita de B, de modo que $AN = \frac{s+1}{r} \cdot u$.

Isso sugere que se chame cada racional $\frac{s}{r}$ nessas condições de *aproximação por falta da medida de* AB e cada $\frac{s+1}{r}$ de *aproximação por excesso da medida de* AB.

Destacaremos duas propriedades das aproximações por falta da medida de um segmento de reta AB:

- Se $\frac{s}{r}$ é uma delas e se $0 < \frac{m}{n} < \frac{s}{r}$, então:

$$\frac{m}{n} \cdot u < \frac{s}{r} \cdot u < AB$$

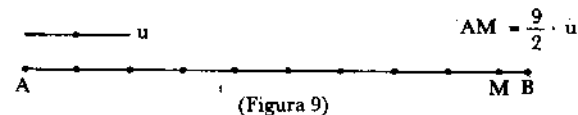
e portanto $\frac{m}{n}$ também é uma aproximação por falta da medida de AB.

- Se $\frac{s}{r}$ é uma aproximação racional por falta da medida de AB, então existem $\frac{m}{n} \in \mathbb{Q}$ de modo que:

$$\frac{s}{r} \cdot u < \frac{m}{n} \cdot u < AB$$

Ou seja, sempre é possível obter aproximações racionais por falta cada vez melhores da medida de AB.

Para provarmos esse resultado, seja M em AB o ponto tal que $AM = \frac{s}{r} \cdot u$ (fig. 9). Isso posto, tomemos $n \in \mathbb{N}^*$ de maneira que

(Figura 9)

$n \cdot MB > u$ ($\iff \frac{1}{n} \cdot u < MB$) e seja m o menor natural não nulo que verifica

$$m \cdot \left(\frac{1}{n} \cdot u\right) = \frac{m}{n} \cdot u > AM$$

Logo, $\frac{m-1}{n} \cdot u < AM$. Então:

$$\frac{m}{n} \cdot u > \frac{s}{r} \cdot u \quad \left(\text{pois } AM = \frac{s}{r} \cdot u\right)$$

e

$$\frac{m}{n} \cdot u = \frac{m-1}{n} \cdot u + \frac{1}{n} \cdot u < AM + MB = AB$$

Poder-se-ia provar ainda, de maneira parecida, que se $\frac{s}{r}$ é uma aproximação racional por excesso da medida de AB, então existem m, n $\in \mathbb{N}^*$ de maneira que $\frac{m}{n} < \frac{s}{r}$ e $\frac{m}{n}$ também é uma aproximação por excesso da medida de AB.

Exemplo 1: Consideremos um quadrado de lado 1 (logo, a unidade de comprimento é congruente ao lado). Pelo teorema de Pitágoras (ver figura 7) a medida d de sua diagonal é $d = \sqrt{2}$ ($\iff d^2 = 2$). Os números

$$1;\ 1{,}4;\ 1{,}41;\ 1{,}414;\ \ldots$$

são aproximações racionais por falta da medida da diagonal, pois:

$$1^2 = 1 < 2;\ (1{,}4)^2 = 1{,}96 < 2;\ (1{,}41)^2 = 1{,}9881 < 2;\ \ldots$$

E os números

$$2;\ 1{,}5;\ 1{,}42;\ 1{,}415;\ \ldots$$

são aproximações por excesso.

2. Cortes em $\mathbb{Q}$

Seja $A \subset \mathbb{Q}$, $A \neq \emptyset$. Um elemento $a \in A$ é chamado *mínimo* de A se $a \leqslant x$, para todo $x \in A$. A propriedade anti-simétrica da relação $\leqslant$ garante que um subconjunto não vazio $A \subset \mathbb{Q}$ não pode ter mais que um mínimo. Notação: $a = \min A$.

Por exemplo, se $A = \mathbb{N}$, então o mínimo de A é 0. O conjunto $A = \{x \in \mathbb{Q} \mid 0 < x < 1\}$ não tem mínimo pelo fato de que, para todo $x \in \mathbb{Q}$:

$$0 < x < 1 \Rightarrow 0 < \frac{1}{2}x < x < 1$$

(ver cap. IV, 3.5).

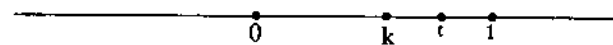
Uma *cota superior* de um subconjunto não vazio $B \subset \mathbb{Q}$ é um número racional k tal que $k \geqslant x$, para todo $x \in B$. Por exemplo, todo número racional $\geqslant 1$ é cota superior de $B = \{x \in \mathbb{Q} \mid -1 < x < 1\}$. Diz-se que $B \subset \mathbb{Q}$, $B \neq \emptyset$, é *limitado superiormente* se B admite uma (e portanto infinitas) cota superior em $\mathbb{Q}$. Se o conjunto das cotas superiores de $B \subset \mathbb{Q}$, $B \neq \emptyset$, tem um mínimo s, este é chamado *supremo* de B. Notação: $s = \sup B$.

Um elemento c de um conjunto não vazio $C \subset \mathbb{Q}$ se diz *máximo* de C se, para todo $x \in C$, $x \leqslant c$. A propriedade anti-simétrica da relação $\leqslant$ garante também que C não pode ter mais que um máximo. Notação: $c = \max C$.

Exemplo 2: Consideremos $B = \{x \in \mathbb{Q} \mid 0 < x < 1\}$. Primeiro notemos que B não possui máximo já que:

$$0 < x < 1 \Rightarrow 0 < x < \frac{1}{2}(x+1) < 1$$

(cap. IV, 3.5).

Mostremos porém que $1 = \sup B$. É imediato primeiro que 1 é cota superior de B. Mas haverá alguma cota superior de B menor que 1? Vamos supor que sim e seja k uma delas. O fato de $\mathbb{Q}$ ser denso garante que existe $t \in \mathbb{Q}$, $k < t < 1$. Assim:

$t \in B$ (pois $t > 0$) e $t > k$, o que não é possível, pois k é cota superior de B. Logo, $1 = \sup B$.

A definição a seguir é inspirada nas propriedades apontadas no item anterior para o conjunto das aproximações racionais por falta da medida de um segmento de reta. Dela sairá o conceito de número real.

DEFINIÇÃO 1 Um conjunto $\alpha \subset \mathbb{Q}$ recebe o nome de *corte* em $\mathbb{Q}$ se

i $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$
ii Se $x \in \alpha$ e $y < x$, então $y \in \alpha$
iii Para todo $x \in \alpha$ existe $y \in \alpha$ de maneira que $y > x$.

Exemplo 3: Para todo $a \in \mathbb{Q}$ o conjunto $\varrho(a) = \{x \in \mathbb{Q} \mid x < a\}$ é um corte em $\mathbb{Q}$.

Obviamente, $\varrho(a) \neq \emptyset$ e $\varrho(a) \neq \mathbb{Q}$. Se $x \in \varrho(a)$, então $x < a$ e portanto, para todo $y < x$, vale a relação $y < a$, o que significa que $y \in \varrho(a)$. Por últi-

mo, se $x \in \varrho(a)$ então $x < a$, e como $\mathbb{Q}$ é denso, existe $y \in \mathbb{Q}$ de maneira que $x < y < a$. O fato de y ser menor que a garante que $y \in \varrho(a)$, pois y é racional.

Para todo $a \in \mathbb{Q}$ o conjunto $\varrho(a)$ é chamado *corte racional*. Mas nem todos os cortes são racionais, como veremos a seguir.

Exemplo 4: Mostremos que o conjunto

$$\alpha = \{x \in \mathbb{Q} \mid x < 0 \text{ ou } (x \geqslant 0 \text{ e } x^2 < 2)\}$$

é um corte em $\mathbb{Q}$.

É claro que $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$. Se $x \in \alpha$ e $x \leqslant 0$, então

$$y < x \Rightarrow y < 0$$

e portanto $y \in \alpha$. Se $x > 0$ e $x^2 < 2$, então há duas possibilidades para um elemento $y < x$: $y \leqslant 0$, caso em que obviamente $y \in \alpha$ e $0 < y < x$, hipótese da qual decorre que $y^2 < x^2 < 2$ e portanto também se pode concluir que $y \in \alpha$.

Seja $x \in \alpha$. Se $x \leqslant 0$, tomando por exemplo $y = 1$, então $y \in \alpha$ e $y > x$. Consideremos agora $x \in \alpha$ tal que $x > 0$ e $x^2 < 2$. Tomando $h = 2 - x^2$, então $x^2 + h = 2$ e $0 < h < 2$. Seja:

$$y = x + \frac{h}{5}$$

Então:

$$y^2 = \left(x + \frac{h}{5}\right)^2 = x^2 + \frac{2xh}{5} + \frac{h^2}{25}$$

Como $x < 2$ (pois $x^2 < 2$), então $2xh < 4h$. Por outro lado, de $0 < h < 2$ decorre que $h^2 < 2h$. Levando estas relações para a igualdade anterior:

$$y^2 < x^2 + \frac{4h}{5} + \frac{2h}{25} = x^2 + \frac{22h}{25} < x^2 + h = 2$$

Como $y > 0$, isto prova que $y \in \alpha$. Mas $y > x$ (pois $y = x + \frac{h}{5}$), o que conclui a demonstração.

Exemplo 5: Provemos que o corte α, definido no exemplo anterior, não admite supremo em $\mathbb{Q}$.

Observemos antes que todo corte racional $\varrho(a)$ admite supremo em $\mathbb{Q}$: é o elemento a, e a demonstração desse fato segue a mesma idéia do exemplo 2.

Admitamos que $s \in \mathbb{Q}$ seja o supremo de α. Como já vimos, não pode ocorrer $s^2 = 2$. E se $s^2 < 2$, levando em conta que $s > 0$ (pois α contém elementos estritamente positivos), o raciocínio da parte final do exemplo anterior garante que existe $y \in \alpha$ de modo que $y > 0$, $y^2 < 2$ e $s < y$, o que não é possível pois $s = \sup \alpha$. Sobra a hipótese $s^2 > 2$.

Esta última relação implica que $s^2 = 2 + k$, onde $0 < k < 2$. De fato, como s é a menor das cotas superiores de α e 2 é uma cota superior de α, então $s < 2$ e daí $s^2 = 2 + k < 4$, o que implica $k < 2$.

Seja $z = s - \frac{k}{4}$. Então:

$$z^2 = \left(s - \frac{k}{4}\right)^2 = s^2 - \frac{sk}{2} + \frac{k^2}{16} > s^2 - \frac{sk}{2}$$

Mas de $s < 2$ segue $sk < 2k$ e portanto $-\frac{sk}{2} > -k$. Donde:

$$z^2 > s^2 - \frac{sk}{2} > s^2 - k = 2$$

Observemos que como $k < 2$, então $\frac{k}{4} < \frac{1}{2} < s$ e portanto $z = s - \frac{k}{4} > 0$; obviamente vale também $z < s$ pois $z = s - \frac{k}{4}$. Considerando que $z^2 > 2$, então z é uma cota superior de α, o que é absurdo, pois $z < s = \sup \alpha$.

EXERCÍCIOS

415. Prove que a altura e o lado de um triângulo equilátero são segmentos de reta incomensuráveis.

416. Sejam $A = \left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots, \frac{n}{n+1}, \ldots\right\}$ e $B = \left\{-1, -\frac{1}{2}, -\frac{1}{3}, \ldots\right\}$. Mostre que $\sup A = 1$ e $\sup B = 0$.

Resolução (primeira parte): Obviamente 1 é cota superior de A, pois $\frac{n}{n+1} < 1$ para todo $n \in \mathbb{N}$. Seja $\varepsilon \in \mathbb{Q}$, $\frac{1}{2} < \varepsilon < 1$. Como $\mathbb{Q}$ é arquimediano, existe $n \in \mathbb{N}^*$, para o qual se verifica $n \cdot 1 = n > \frac{\varepsilon}{1 - \varepsilon}$; daí $n - n\varepsilon > \varepsilon$ ou $n > (n+1)\varepsilon$ e, portanto, $\frac{n}{n+1} > \varepsilon$. Assim, nenhum racional $\varepsilon < 1$ é cota superior de A, o que conclui a resolução.

417. Se um subconjunto não vazio $A \subset \mathbb{Q}$ admite máximo, prove que $\sup A = \max A$.

418. a) A quais dos cortes seguintes pertencem os números racionais -10, 0, $\frac{2}{3}$, $\frac{5}{2}$, 20: $\varrho(3)$, $\varrho(-1)$, $\varrho(20{,}1)$; $\varrho\left(\frac{1}{4}\right)$?

b) Ache cinco números racionais que pertençam ao corte $\varrho\left(\frac{1}{4}\right)$ mas não pertençam a $\varrho(0)$.

419. Prove que: $\varrho(r) \subset \varrho(s) \iff r < s$.

420. Sejam α e β cortes em $\mathbb{Q}$ tais que existe $b \in \beta$, $b \notin \alpha$. Prove que $\alpha \subsetneq \beta$ ($\alpha \subset \beta$ e $\alpha \neq \beta$).

421. Seja α um corte em $\mathbb{Q}$. Prove que também são cortes em $\mathbb{Q}$:

a) $\beta = \{r + a \mid a \in \alpha\}$, para todo $r \in \mathbb{Q}$.

b) $\gamma = \{ra \mid a \in \alpha\}$, para todo $r \in \mathbb{Q}$, $r > 0$.

Resolução de b): **i** Que $\gamma \neq \emptyset$ é imediato. Como α é um corte, existe $x \in \mathbb{Q}$ tal que $x \notin \alpha$. Mostremos que $rx \notin \gamma$. De fato, se $rx \in \gamma$, então $rx = ra$, para algum $a \in \alpha$, e portanto (já que $r \neq 0$) $x = a$. Absurdo, pois $x \notin \alpha$. **ii** Seja $x \in \gamma$, $x = ra$ com $a \in \alpha$. Se $y < x$, isto é, $y < ra$, então $\frac{y}{r} < a$, o que garante a relação $\frac{y}{r} \in \alpha$. Fazendo $\frac{y}{r} = a_1 \in \alpha$, então $y = ra_1$, do que segue $y \in \gamma$. **iii**. Seja $x \in \gamma$, $x = ra$, onde $a \in \alpha$. Sendo α um corte, existe $b \in \alpha$ tal que $b > a$. Daí $rb > ra = x$ e, como $rb \in \gamma$, então, de fato, γ é um corte em $\mathbb{Q}$.

422. Se α é um corte em $\mathbb{Q}$, indiquemos por α' o complementar de α em relação a $\mathbb{Q}$.

a) Se $r \in \mathbb{Q}$ e $\beta = \{r + a \mid a \in \alpha\}$, prove que $\beta' = \{r + x \mid x \in \alpha'\}$.

b) Se $r \in \mathbb{Q}$, $r > 0$, e $\gamma = \{ra \mid a \in \alpha\}$, prove que $\gamma' = \{rx \mid x \in \alpha'\}$.

423. Seja α um corte em $\mathbb{Q}$.

a) Se $a \in \alpha$, prove que $\varrho(a) \subsetneq \alpha$ ($\iff \varrho(a) \subset \alpha$ e $\varrho(a) \neq \alpha$).

b) Se $a \in \mathbb{Q} - \alpha$ ($\iff a \in \mathbb{Q}$; $a \notin \alpha$), prove que $\alpha \subset \varrho(a)$.

3. Os números reais

O exemplo anterior põe em relevo uma deficiência do corpo ordenado $\mathbb{Q}$: há subconjuntos não vazios de $\mathbb{Q}$, limitados superiormente, que não admitem supremo em $\mathbb{Q}$. O conjunto dos números reais é uma extensão do conjunto dos números racionais, construída com o objetivo de preencher as lacunas de $\mathbb{Q}$ determinadas pela ausência desses supremos.

A idéia que usaremos para chegar a essa extensão de $\mathbb{Q}$ remonta ao matemático grego Eudoxo de Cnido (séc. IV a.C.) e baseia-se na observação de que um "número real" não racional fica determinado pelos números racionais que o precedem.

DEFINIÇÃO 2 Seja $\mathbb{R}$ o conjunto de todos os cortes em $\mathbb{Q}$. Os elementos de $\mathbb{R}$ serão chamados *números reais* e, conseqüentemente, $\mathbb{R}$ será chamado *conjunto dos números reais* desde que as operações *adição* e *multiplicação* e a relação $\leqslant$ em $\mathbb{R}$ sejam definidas da maneira a seguir.

Adição

Se α e β são cortes em $\mathbb{Q}$, a *soma* de α com β é o conjunto

$$\alpha + \beta = \{x + y \mid x \in \alpha,\ y \in \beta\}$$

A soma $\alpha + \beta$ também é um corte em $\mathbb{Q}$. É claro que $\alpha + \beta$ verifica a condição **i** da definição 1. Seja $x + y$ ($x \in \alpha$, $y \in \beta$) um elemento de $\alpha + \beta$ e consideremos um racional $u < x + y$. Então $x + y = u + t$ para um conveniente $t \in \mathbb{Q}$, $t > 0$. Fazendo $y - t = z$, então $y = t + z$ (o que mostra que $z < y$ e portanto $z \in \beta$) e $u = x + z$. Como, porém, $x \in \alpha$ e $z \in \beta$, então $u \in \alpha + \beta$.

Por último, seja $z \in \beta$ tal que $z > y$. Então $x + z > x + y$ e $x + z \in \alpha + \beta$.

Assim, $(\alpha, \beta) \longrightarrow \alpha + \beta$ é uma operação sobre $\mathbb{R}$ à qual chamamos *adição de números reais*. Para essa operação valem as seguintes propriedades (aqui apenas enunciadas):

a_1 $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ (associativa)

a_2 $\alpha + \beta = \beta + \alpha$ (comutativa)

a_3 Existe elemento neutro: é o corte racional $\varrho(0)$ que indicaremos apenas por 0.

a_4 Para todo $\alpha \in \mathbb{R}$ a equação $\alpha + x = 0$ tem uma única solução em $\mathbb{R}$. Essa solução é corte indicado por $-\alpha$ (oposto de α) e que consta de todos os $x \in \mathbb{Q}$ tais que $x + y \in \varrho(0)$, para todo $y \in \alpha$, exceto o maior desses x, caso exista.

Exemplo 6: Mostremos que $\varrho(2) + \varrho(-2) = \varrho(0) = 0$.

Seja $x + y \in \varrho(2) + \varrho(-2)$, onde $x \in \varrho(2)$ e $y \in \varrho(-2)$. Então $x < 2$ e $y < -2$, e daí: $x + y < 2 + (-2) = 0$. Logo $x + y \in \varrho(0)$.

Seja $z \in \varrho(0)$. Então $z < 0$ e $-z = d > 0$. Como

$$z = \left(2 - \frac{1}{2}d\right) + \left(-2 - \frac{1}{2}d\right)$$

onde $2 - \frac{1}{2}d \in \varrho(2)$ e $-2 - \frac{1}{2}d \in \varrho(-2)$, então $z \in \varrho(2) + \varrho(-2)$.

Logo, $\varrho(-2) = -\varrho(2)$. De modo análogo se prova que $\varrho(-a) = -\varrho(a)$, para todo $a \in \mathbb{Q}$.

Relação $\leqslant$

Se $\alpha, \beta \in \mathbb{R}$, então se diz que *$\alpha$ é menor que ou igual a β* e escreve-se $\alpha \geqslant \beta$ se $\alpha \cup \beta$.

Para a relação $\leqslant$ assim definida valem as seguintes propriedades:

O_1 $\alpha \leqslant \alpha$ (reflexiva)

O_2 $\alpha \leqslant \beta$ e $\beta \leqslant \alpha \Rightarrow \alpha = \beta$ (anti-simétrica)

O_3 $\alpha \leqslant \beta$ e $\beta \leqslant \gamma \Rightarrow \alpha \leqslant \gamma$ (transitiva)

O_4 $\alpha \leqslant \beta$ ou $\beta \leqslant \alpha$

Como sempre: $\beta \geqslant \alpha \iff \alpha \leqslant \beta$. Obviamente, por $\alpha < \beta$ entende-se que $\alpha \subset \beta$ e $\alpha \neq \beta$. Neste caso também se pode escrever $\beta > \alpha$. Os conceitos de positivo, estritamente positivo, negativo e estritamente negativo são definidos da maneira habitual. É imediato que: $r \in \alpha \Rightarrow \varrho(r) < \alpha$.

Exemplo 7: Mostremos que $\alpha \in \mathbb{R}$ é estritamente positivo se, e somente se, existe $x \in \mathbb{Q}$ tal que $x > 0$ e $x \in \alpha$.

Se $\alpha > 0 = \varrho(0)$, então $\varrho(0) \subset \alpha$ e $\varrho(0) \neq \alpha$. Assim existe $y \in \alpha$ tal que $y \notin \varrho(0)$. Desta última relação segue que $y \geqslant 0$. Se $y > 0$, a demonstração está encerrada. Se $y = 0$, o item **iii** da definição de corte garante que existe $x \in \alpha$, $x > 0$.

Reciprocamente, se existe $x \in \alpha$, $x > 0$, como todo racional $y < x$ pertence a α, devido à condição **ii** da citada definição, podemos garantir que $\varrho(0) \underset{\neq}{\subset} \alpha$ e, portanto, $0 < \alpha$ (pois $x \in \alpha$ e $x \notin \varrho(0)$).

Multiplicação

Se α e β são elementos de $\mathbb{R}$, então o *produto* $\alpha\beta$ (ou $\alpha \cdot \beta$) é definido assim:

- Se $\alpha > 0$ e $\beta > 0$, então:

$$\alpha\beta = \{x \in \mathbb{Q} \mid x \leqslant 0\} \cup \{xy \mid x \in \alpha,\ x > 0;\ y \in \beta,\ y > 0\}$$

- Se $\alpha = 0$ ou $\beta = 0$, $\alpha\beta = 0$
- Se $\alpha < 0$ e $\beta < 0$, então $\alpha\beta = (-\alpha)(-\beta)$
- Finalmente, se apenas um dos cortes é menor que zero, digamos $\alpha < 0$ e $\beta \geqslant 0$, então:

$$\alpha\beta = -(-\alpha)\beta$$

Fica como exercício provar que $(\alpha, \beta) \rightarrow \alpha\beta$ é uma operação sobre $\mathbb{R}$. Trata-se da *multiplicação de números reais* e para ela são válidas as seguintes propriedades:

m_1 $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ (associativa)

m_2 $\alpha\beta = \beta\alpha$ (comutativa)

m_3 Existe elemento neutro: é o corte racional $\varrho(1)$, que indicaremos apenas por 1.

m_4 Para todo $\alpha \in \mathbb{R}$, $\alpha \neq 0$, a equação $\alpha \cdot \chi = 1$ tem uma única solução em $\mathbb{R}$. Essa solução chama-se inverso de α e é indicada por α^{-1}.

d Distributiva em relação à adição: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$, para quaisquer $\alpha, \beta, \gamma \in \mathbb{R}$.

Omitiremos as demonstrações dessas propriedades. Trata-se de tarefa um tanto árida e não é o que mais importa aqui. Por isso só nos deteremos para demonstrações em coisas mais específicas de $\mathbb{R}$. Registremos ainda que a relação $\leqslant$ é compatível com a adição e a multiplicação de $\mathbb{R}$, ou seja:

O_5 $\alpha \leqslant \beta \Rightarrow \alpha + \gamma \leqslant \beta + \gamma$

O_6 $\alpha \leqslant \beta$ e $0 \leqslant \gamma \Rightarrow \alpha\gamma \leqslant \beta\gamma$

A esta altura podemos concluir que $\mathbb{R}$, tal como $\mathbb{Q}$, é um corpo ordenado. As peculiaridades do corpo ordenado dos números reais aparecerão em pouco.

Outro fato que apenas nos limitaremos a citar é que $f: \mathbb{Q} \rightarrow \mathbb{R}$ definida por $f(a) = \varrho(a)$:

- é injetora
- conserva as operações de adição e multiplicação, o que significa:

$$f(a + b) = f(a) + f(b)\ (\iff \varrho(a + b) = \varrho(a) + \varrho(b))$$
$$f(ab) = f(a)f(b)\ (\iff \varrho(ab) = \varrho(a)\varrho(b))$$

- conserva as relações de ordem, ou seja:

$$a \leqslant b \Rightarrow f(a) \leqslant f(b)$$

ou

$$a \leqslant b \Rightarrow \varrho(a) \leqslant \varrho(b)$$

Portanto, é valido identificar cada $a \in \mathbb{Q}$ com o corte $\varrho(a)$ e assim considerar $\mathbb{Q} \subset \mathbb{R}$ (enquanto corpos ordenados). Daqui para a frente, portanto, faremos $\varrho(a) = a$ ($\forall a \in \mathbb{Q}$), sempre que for conveniente. A função f é chamada *função imersão* de $\mathbb{Q}$ em $\mathbb{R}$. Na identificação proporcionada por f, os elementos $\varrho(a)$ passam a ser chamados *números racionais* e os de $I = \mathbb{R} - \mathbb{Q}$ *números irracionais*. O corte α do exemplo 4 é um número irracional.

Exemplo 8: Sejam $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$. Mostremos que existe $\gamma \in \mathbb{R}$ de modo que $\beta = \alpha + \gamma$ ($\gamma > 0$).

Por hipótese, $\alpha \subset \beta$ e $\alpha \neq \beta$. Assim, se α' é o complementar de α em relação a $\mathbb{Q}$, ou seja, $\alpha' = \{x \in \mathbb{Q} \mid x \notin \alpha\}$, então $\alpha' \cap \beta \neq \varnothing$. Seja a um racio-

nal dessa intersecção ($a \in \alpha' \cap \beta$) e consideremos $b \in \beta$, $b > a$, o que implica $-b < -a$. Mostremos que $-b \in -\alpha$. De fato, para todo $y \in \alpha$ tem-se $y < a$ (pois $a \in \alpha'$) e portanto (levando em conta que $-b < -a$):

$$-b + y < -a + y < -a + a = 0$$

ou seja, $-b + y \in \varrho(0)$, o que prova nossa afirmação.

Como porém $-\alpha$ é um corte, então existe $c \in (-\alpha)$, $c > -b$. Daí $c + b > 0$. Mas considerando que $b + c \in \beta + (-\alpha)$, então $\beta + (-\alpha) > 0 = \varrho(0)$. Fazendo $\beta + (-\alpha) = \beta - \alpha = \gamma$ (pois $\beta + (-\alpha)$ é um corte), então $\beta = \alpha + \gamma$, onde $\gamma > 0$, pois $b + c \in \gamma$.

Nota:

i Como já vimos, IR é um corpo ordenado. Assim, todas as propriedades que valem para $\mathbb{Q}$, enquanto corpo ordenado, como as que aparecem no capítulo IV, também valem em IR. Daí por que várias dessas últimas nem sequer são citadas aqui, embora eventualmente possamos usar uma ou outra sem qualquer menção explícita. Por exemplo, a definição de potência m-ésima ($m \in \mathbb{Z}$) de um número real α é análoga à que foi dada no exemplo 1 (cap. IV) e para ela valem as mesmas propriedades que lá figuram.

ii Daqui para a frente, sempre que for conveniente, usaremos também letras minúsculas de nosso alfabeto para indicar números reais.

Exemplo 9: Seja q, $0 < q < 1$, um número real. Mostremos que: $0 \leqslant m \leqslant n \Rightarrow 0 < q^n \leqslant q^m$

Provaremos, por indução sobre m, que

$$0 < q^{m+1} < q^m \ (\forall m \geqslant 0)$$

$m = 0$: $0 < q^1 < q^0$ ou $0 < q < 1$ (verdadeira)

Seja $r \geqslant 0$ e suponhamos $0 < q^{r+1} < q^r$. Como $q > 0$, então

$$0 \cdot q < q^{r+1} \cdot q < q^r \cdot q$$

ou seja:

$$0 < q^{(r+1)+1} < q^{r+1}$$

Conseqüentemente:

$$0 < \ldots < q^{m+3} < q^{m+2} < q^{m+1} < q^m$$

Por outro lado é claro que, se $m = n \geqslant 0$, então $q^n = q^m$.

Exemplo 10 (*desigualdade de Bermoulli*): Provemos que, para todo número real $a \geqslant -1$ e todo número natural $n \geqslant 1$, vale a desigualdade:

$$(1 + a)^n \geqslant 1 + na$$

Por indução sobre n:

$n = 1$: $(1 + a)^1 = 1 + a = 1 + 1 \cdot a$. Verdadeira.

Seja $r \geqslant 1$ e suponhamos $(1 + a)^r \geqslant 1 + ra$.

$n = r + 1$: Multipliquemos a desigualdade anterior (hipótese de indução) por $1 + a \geqslant 0$:

$$(1 + a)^{r+1} \geqslant (1 + ra)(1 + a) = 1 + ra + a + ra^2$$

Como $ra^2 \geqslant 0$, então:

$$1 + ra + a + ra^2 \geqslant 1 + ra + a = 1 + (r + 1)a$$

Donde:

$$(1 + a)^{r+1} \geqslant 1 + (r + 1)a$$

PROPOSIÇÃO 1 Sejam $\alpha, \beta \in$ IR, $\alpha > 0$. Então existe $n \in$ IN* de maneira que $n\alpha > \beta$. (Ou seja: o corpo ordenado IR é arquimediano.)

Demonstração: Podemos nos ater ao caso $\beta > \alpha$. Como $\alpha > 0$, então $\beta > 0$ e, portanto, existem racionais estritamente positivos r e s tais que $r \in \alpha$ e $s \notin \beta$. Sendo $\mathbb{Q}$ arquimediano, então

$$nr > s$$

para algum $n \in$ IN*. Considerando a imersão de $\mathbb{Q}$ em IR, a desigualdade anterior pode ser expressa por:

$$\varrho(n)\varrho(r) = \varrho(nr) > \varrho(s)$$

Como porém $r \in \alpha$, então $\varrho(r) \subset \alpha$, o que pode ser traduzido por $\alpha \geqslant \varrho(r)$. Mas, considerando que $\varrho(n) > 0$ (pois $\varrho(n) = n$), então:

$$\varrho(n)\alpha \geqslant \varrho(n)\varrho(r)$$

Por outro lado, em virtude da escolha de s, é claro que $\varrho(s) \geqslant \beta$. Donde:

$$n\alpha = \varrho(n)\alpha \geqslant \varrho(n)\varrho(r) > \varrho(s) \geqslant \beta. \qquad \blacksquare$$

Exemplo 11: Seja a, $0 < a < 1$, um número real. Mostremos que para todo $\varepsilon \in$ IR, $\varepsilon > 0$, existe $n \in$ IN* de maneira que $a^n < \varepsilon$.

Uma vez que $0 < a < 1$, então $b = a^{-1} > 1$. Logo $b = 1 + h$, para algum $h \in$ IR, $h > 0$. Devido ao fato de IR ser arquimediano, existe $n \in$ IN* para o qual

$$nh > \varepsilon^{-1} - 1$$

e portanto:

$$nh + 1 > \varepsilon^{-1}$$

Mas, devido à desigualdade de Bernoulli:

$$b^n = (1 + h)^n \geqslant 1 + nh$$

Portanto:

$$(a^{-1})^n = b^n = (1 + h)^n \geqslant 1 + nh > \varepsilon^{-1}$$

Mas

$$(a^{-1})^n = (a^n)^{-1}$$

e, então:

$$(a^n)^{-1} > \varepsilon^{-1}$$

Donde:

$$a^n < \varepsilon$$

PROPOSIÇÃO 2 Sejam $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$. Então existe um número racional r tal que $\alpha < r < \beta$.

Demonstração: Como $\alpha < \beta$, então $\alpha \subsetneq \beta$ ($\alpha \subset \beta$ e $\alpha \neq \beta$) e, portanto, existe $s \in \beta$ tal que $s \notin \alpha$. Seja $r \in \beta$ um número racional maior que s e mostremos que $\alpha \leqslant s < r < \beta$, ou seja, que $\alpha \subset \varrho(s) \subsetneq \varrho(r) \subsetneq \beta$.

Suponhamos que existisse $x \in \alpha$ tal que $x \notin \varrho(s)$ ou, equivalentemente, $x \geqslant s$. Como $s \notin \alpha$, então na verdade $s < x$. Mas esta desigualdade implica que $s \in \alpha$, pois $x \in \alpha$ e α é um corte em $\mathbb{Q}$. Absurdo. Donde todo elemento de α está em $\varrho(s)$, o que significa $\alpha \subset \varrho(s)$.

Falta provar que $\varrho(r) \subsetneq \beta$. Se $x \in \varrho(r)$, então $x < r$, e como $r \in \beta$, então $x \in \beta$. Assim: $\varrho(r) \subset \beta$. Por outro lado, levando em conta que $r \in \beta$, resulta que existe $u \in \beta$, $u > r$; daí $\varrho(r) \subsetneq \varrho(u)$ (pois a imersão $y \to \varrho(y)$ é injetora). Como $u \in \beta$ implica $\varrho(u) \subset \beta$, então $\varrho(r) \subsetneq \varrho(u) \subset \beta$ e daí: $\varrho(r) \subsetneq \beta$. Assim:

$$\alpha < \varrho(r) = r < \beta$$ ■

Nota: Seja K um corpo ordenado. Se existe $L \subset K$, $L \neq \varnothing$, de maneira que para quaisquer $x, y \in K$, $x < y$, seja sempre possível determinar $g \in L$ de modo que $x < z < y$, então se diz que L é *denso em* K. É claro que nessas condições K é um corpo ordenado denso. A proposição anterior garante que $\mathbb{Q}$ é denso em $\mathbb{R}$ e que portanto $\mathbb{R}$ é denso. Também se pode provar (veja exercício número 446) que o conjunto I dos números irracionais é denso em $\mathbb{R}$.

Seja $A \subset \mathbb{R}$, $A \neq \varnothing$. Um elemento $\lambda \in \mathbb{R}$ é uma *cota superior* de A se $\alpha \leqslant \lambda$, para todo $\alpha \in A$. Se A admite cota superior em $\mathbb{R}$, diz-se que A é *limitado superiormente*. Neste caso, como mostraremos a seguir, o conjunto das cotas

superiores de A tem um mínimo λ_0. Ou seja: **i** $\alpha \leqslant \lambda_0$, $\forall \alpha \in A$; **ii** se $\alpha \leqslant \lambda$, $\forall \alpha \in A$, então $\lambda_0 \leqslant \lambda$. O elemento λ_0 (que é único devido à anti-simetria de $\leqslant$) chama-se *supremo* de A. Notação $\lambda_0 = \sup A$.

TEOREMA 1 Seja $A \subset \mathbb{R}$, $A \neq \varnothing$. Se A é limitado superiormente, então A admite supremo em $\mathbb{R}$.

Demonstração: Seja $\lambda_0 = \bigcup_{\alpha \in A} \alpha$ e mostremos inicialmente que λ_0 é um corte em $\mathbb{Q}$, ou seja, $\lambda_0 \in \mathbb{R}$. Como cada $\alpha \neq \varnothing$, então evidentemente $\lambda_0 \neq \varnothing$; se λ é uma cota superior de A, então $\alpha \subset \lambda$, $\forall \alpha \in A$, e tomando $x \in \mathbb{Q}$ tal que $x \notin \lambda$, então x não pertence a nenhum dos $\alpha \in A$ e daí $x \notin \lambda_0$. Provamos assim que vale para λ_0 a condição **i** da definição 1.

Se $x \in \lambda_0$, então $x \in \alpha$, para algum $\alpha \in A$; assim, se $y \in \mathbb{Q}$ e $y < x$, então $y \in \alpha$ e portanto $y \in \lambda_0$. Logo λ_0 verifica também o item **ii** da citada definição.

Quanto à **iii**, notemos que se $x \in \lambda_0$, como então $x \in \alpha$, para algum $\alpha \in A$, tomando $y \in \alpha$, $y > x$, então $y \in \lambda_0$.

Mostremos agora que $\lambda_0 = \sup A$. Primeiro, como $\alpha \subset \lambda_0$, para todo $\alpha \in A$, então $\alpha \leqslant \lambda_0$, $\forall \alpha \in A$. E se λ é um número real que é cota superior de A, isto é, $\alpha \leqslant \lambda$, para todo $\alpha \in A$, então $\alpha \subset \lambda$ (para qualquer $\alpha \in A$) e portanto:

$$\lambda_0 = \bigcup_{\alpha \in A} \alpha \subset \lambda$$

Ou seja: $\lambda_0 \leqslant \lambda$. ■

Nota: Como já dissemos, tanto $\mathbb{Q}$ como $\mathbb{R}$ são corpos ordenados. Mas enquanto no primeiro há subconjuntos não vazios e limitados superiormente que não admitem supremo em $\mathbb{Q}$ (exemplo 5), o mesmo não acontece em $\mathbb{R}$ — o que é provado pelo teorema anterior. Para assinalar essa diferença dizemos que $\mathbb{R}$ é um *corpo ordenado completo*. Portanto, o corpo ordenado $\mathbb{Q}$ não é completo.

O corpo ordenado $\mathbb{R}$ também é *contínuo* no sentido de que vale o corolário a seguir (na verdade, equivalente ao teorema 1).

COROLÁRIO Sejam A e B subconjuntos de $\mathbb{R}$ tais que $A \cup B = \mathbb{R}$ e, ainda, que todo $a \in A$ é menor que todo $b \in B$. Então existe um único $c \in \mathbb{R}$ que não é superado por nenhum $a \in A$ e que não supera nenhum $b \in B$.

Demonstração: Todo $b \in B$ é cota superior de A, de modo que existe $c = \sup A$, $c \in \mathbb{R}$. Logo $a \leqslant c$, para todo $a \in A$. Mas como todo $b \in B$ é cota superior de A e c é a menor dessas cotas, então $c \leqslant b$, qualquer que seja $b \in B$. Isto conclui a demonstração quanto à existência.

Suponhamos que um outro número real d gozasse da mesma propriedade já demonstrada para c. Admitamos, por exemplo, que $c < d$. Considerando a média aritmética

$$\frac{c + d}{2} = u$$

então u não pertence à classe A (por ser maior que c) e também não pertence a B (por ser menor que d). Mas isto é absurdo, uma vez que $A \cup B = \mathbb{R}$ e $u \in \mathbb{R}$. ■

Exemplo 12: Mostremos que em $\mathbb{R}$ existe um número elemento $c > 0$ tal que $c^2 = 2$.

Provaremos apenas a existência.

Sejam:

$$A = \{a \in \mathbb{R} \mid a < 0 \text{ ou } (a \geqslant 0 \text{ e } a^2 < 2)\}$$

e

$$B = \{b \in \mathbb{R} \mid b > 0 \text{ e } b^2 \geqslant 2\}$$

Seja $x \in \mathbb{R}$. Se $x \leqslant 0$, então $x \in A$.

Se $x > 0$, então: $x^2 < 2$ ou $x^2 = 2$, ou $x^2 > 2$. Na primeira hipótese $x \in A$; nas duas segundas $x \in B$. Logo $A \cup B = \mathbb{R}$.

Por outro lado, seja $a \in A$. Se $a \leqslant 0$, então obviamente a é menor que todo $b \in B$. Se $a > 0$, então $a^2 < 2$ e como $b^2 \geqslant 2$, para todo $b \in B$, podemos concluir que $a^2 < b^2$ e daí que $a < b$. Assim: $a < b$, sempre que $a \in A$ e $b \in B$.

Devido as corolário anterior existe um único $c \in \mathbb{R}$ de modo que $a \leqslant c \leqslant b$, para qualquer $a \in A$ e qualquer $b \in B$. Mostraremos agora, por redução, ao absurdo, que $c^2 = 2$. (Obviamente $c > 0$.)

Vamos supor que se pudesse ter $c^2 > 2$. Como $c \in \mathbb{R}$, a definição de produto $c^2 = c \cdot c$ garante a existência de dois números racionais estritamente positivos x e y de modo que $2 < xy < c^2$ (na verdade x e y pertencem ao corte c). Supondo $x \leqslant y$, então $xy \leqslant y^2$ e portanto $2 < y^2$, de onde se conclui que $y \in B$. Mas $y < c$, pois $y \in c$. Absurdo uma vez que c não supera nenhum elemento de B.

Analogamente se prova que a hipótese $c^2 < 2$ é impossível. Donde $c^2 = 2$.

O número real c tal que $c^2 = 2$ é chamado raiz quadrada de 2 e é indicado por $\sqrt{2}$. De forma análoga ao que foi feito neste exemplo pode-se mostrar que, dados $a, n \in \mathbb{N}^*$, $n \geqslant 2$, existe um único $c > 0$ para o qual vale

$$c^n = a$$

Esse número é chamado *raiz enésima* de a e é indicado por $\sqrt[n]{a}$.

3.1 Valor absoluto (ou módulo)

O conceito de *valor absoluto* ou *módulo* em $\mathbb{R}$ é essencialmente o mesmo que em $\mathbb{Z}$ ou $\mathbb{Q}$. Assim, denotando por $|a|$ o valor absoluto de $a \in \mathbb{R}$, por definição

$$|a| = a \text{ se } a \geqslant 0$$
$$|a| = -a \text{ se } a < 0$$

Todas as propriedades que figuram na proposição 4, capítulo IV, também valem quando as letras com que são expressas passam a representar números reais. Demonstrá-las, inclusive, seria mera repetição — por isso não o faremos aqui. A seguinte propriedade (também válida quando se troca $\mathbb{R}$ por $\mathbb{Z}$ ou $\mathbb{Q}$) será usada no item 5.

- Se $x, a, \varepsilon \in \mathbb{R}$, $\varepsilon > 0$, então:

$$|x - a| < \varepsilon \iff a - \varepsilon < x < a + \varepsilon$$

Prova

$\Rightarrow$ Vamos supor $x - a \geqslant 0$. Então $|x - a| = x - a < \varepsilon$ e daí $x < a + \varepsilon$. Como porém $\varepsilon > 0$, então $-\varepsilon < 0$ e portanto $a - \varepsilon < a$. Mas como $x - a \geqslant 0$, então $a \leqslant x$. Assim:

$$a - \varepsilon < a \leqslant x < a + \varepsilon$$

Deixamos como exercício o caso $x - a < 0$.

$\Leftarrow$ Somando $-a$ a cada um dos termos de $a - \varepsilon < x < a + \varepsilon$ (hipótese), obtém-se

$$-\varepsilon < x - a < \varepsilon$$

Se $x - a \geqslant 0$, então $|x - a| = x - a < \varepsilon$. Se $x - a < 0$, então $|x - a| = a - x$; mas de $-\varepsilon < x - a$ segue que $a - x < \varepsilon$; logo $|x - a| < \varepsilon$. ■

3.2 Função maior inteiro

Também não há nenhuma novidade essencial, em relação a $\mathbb{Q}$, para conceituar a *função maior inteiro* em $\mathbb{R}$. O *maior inteiro contido* em $a \in \mathbb{R}$ (notação $[a]$) é definido por:

i $[a] \in \mathbb{Z}$

ii $[a] \leqslant a$

iii Se m é inteiro e $m \leqslant a$, então $m \leqslant [a]$.

A lei $x \to [x]$ define a função maior inteiro cujo domínio é $\mathbb{R}$ e cujo conjunto-imagem é $\mathbb{Z}$.

Notemos que se $a \in \mathbb{R}$ e m é um inteiro tal que $m \leqslant a < m + 1$, então $m = [a]$ (justifique).

As propriedades enunciadas na proposição 5, capítulo IV, também valem quando se substitui $\mathbb{Q}$ por $\mathbb{R}$. Inclusive as demonstrações são basicamente as mesmas.

EXERCÍCIOS

424. Prove que são irracionais os números $\sqrt{3}$, $\sqrt{5}$ e $\sqrt{7}$.

Resolução: Suponhamos que se pudesse ter $\sqrt{3} = \frac{r}{s}$ ($r, s \in \mathbb{N}$; $s \neq 0$). Então $r^2 = 3s^2$. Mas nesta igualdade o expoente de 3 no primeiro membro é par ($\geqslant 0$) e no segundo é ímpar ($\geqslant 1$), o que contraria o teorema fundamental da aritmética (unicidade).

425. Seja $p > 1$ um número primo. Prove que $\sqrt{p}$ é irracional.

426. Prove que a soma de um número racional com um irracional é irracional.

Sugestão: Por absurdo, suponha que pudesse ser racional.

427. Prove que o produto de um número racional não nulo por um irracional é um número irracional.

428. Exiba dois números irracionais distintos cuja diferença seja racional.

429. Exiba dois irracionais distintos cujo quociente seja racional.

430. Sejam $\alpha, \beta \in \mathbb{R}$ números tais que $\beta^2 = \alpha$. Mostre que se α é irracional, o mesmo acontece com β. (Neste caso usa-se a notação $\beta = \sqrt{\alpha}$.)

Resolução: Se β fosse racional, então $\beta^2 = \beta \cdot \beta = \alpha$ também seria, o que é absurdo.

431. Sejam α e β irracionais. Se $\alpha + \beta$ é racional, prove que $\alpha - \beta$ é irracional.

Resolução: Se $\alpha - \beta$ fosse racional, então $(\alpha + \beta) + (\alpha - \beta) = 2\alpha$ também seria pois $\alpha + \beta \in \mathbb{Q}$, por hipótese. Mas então $\frac{2\alpha}{2} = \alpha$ também teria que ser racional, o que contraria a hipótese.

432. Sejam α e β irracionais. Se $\alpha - \beta$ é racional, prove que $\alpha + 2\beta$ é irracional.

433. Prove que $\sqrt{2} + \sqrt{3}$ é irracional.

Resolução: Seja $u = \sqrt{2} + \sqrt{3}$. Então $u - \sqrt{2} = \sqrt{3}$ e portanto $u^2 - 2\sqrt{2}\,u + 2 = 3$. Daí $2\sqrt{2}\,u = u^2 - 1$, do que resulta (elevando ao quadrado): $8u^2 = u^4 - 2u^2 + 1$ ou $u^4 - 10u^2 + 1 = 0$. Logo u é raiz do polinômio $f(x) = x^4 - 10x^2 + 1$ cujos coeficientes são inteiros. Mas, de acordo com o exercício 387, as possíveis raízes de f(x) são ± 1 (os divisores de 1). Como $f(1) = f(-1) = -8$, f(x) não admite raízes racionais e portanto $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

434. Prove que são irracionais: $\sqrt{3} - \sqrt{2}$, $\sqrt[3]{2} + \sqrt{3}$ e $\sqrt[3]{3} - \sqrt{2}$.

435. Seja $p > 1$ um número primo. Para todo $n \geqslant 2$, prove que $\sqrt[n]{p}$ é irracional.

Sugestão: Usar a idéia apresentada na resolução do exercício 433.

436. Prove que cos 20° é irracional.

Resolução: Consideremos a identidade $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Se $\theta = 20°$, fazendo $\cos\theta = u = \cos 20°$, então

$$\frac{1}{2} = \cos 60° = 4u^3 - 3u$$

e portanto $8u^3 - 6u - 1 = 0$. Assim, $u = \cos 20°$ é raiz de $f(x) = 8x^3 - 6x - 1$. Mas fazendo $2x = y$, então $2u$ é raiz de $g(y) = y^3 - 3y - 1$. Como $g(1) = -3$ e $g(-1) = +1$ então g não admite raízes racionais e portanto $2u$ é irracional. Daí u também é irracional.

437. Prove que são irracionais os números cos 40° e cos 10°.

438. Prove que são irracionais: sen 20° e sen 50°.

439. Use a identidade $\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta$ para mostrar que cos 12° é irracional.

440. Se $\cos 2\theta$ é irracional, prove que coso também é irracional.

Resolução: Se $\cos\theta$ fosse racional, o mesmo aconteceria com $\cos^2\theta$ e $2\cos^2\theta - 1$. Como porém $\cos 2\theta = 2\cos^2\theta - 1$, caímos num absurdo.

441. Se $\cos 2\theta$ é irracional, prove que $\text{sen}\,\theta$ e $\text{tg}\,\theta$ também são irracionais.

442. Prove que se $\cos\theta$ é racional, então $\cos 3\theta$ também é racional.

443. Através do uso conveniente de alguns dos exercícios anteriores, prove que são irracionais os números

$$\cos 10°,\ \text{sen}\ 10°,\ \text{tg}\ 10°$$
$$\cos 5°,\ \text{sen}\ 5°,\ \text{tg}\ 5°$$
$$\cos 2°30',\ \text{sen}\ 2°30',\ \text{tg}\ 2°30'$$

444. Prove que:

a) $\varrho(2) + \varrho(3) = \varrho(5)$

b) $\varrho(2) \cdot \varrho(3) = \varrho(6)$ (sem usar o fato de que $n \rightarrow \varrho(n)$ define a imersão de $\mathbb{Q}$ em $\mathbb{R}$).

Resolução de a): Seja $z \in \varrho(2) + \varrho(3)$. Então $z = x + y$, onde $x \in \varrho(2)$ e $y \in \varrho(3)$, o que equivale a $x < 2$ e $y < 3$. Logo $z = x + y < 2 + 3 = 5$, o que garante a relação $z \in \varrho(5)$. Por outro lado, se $z \in \varrho(5)$, então $z < 5$ e daí $z = 5 - a$, para alguns $a \in \mathbb{Q}$, $a > 0$. Como $z = 5 - a = = \left(2 - \frac{a}{2}\right) + \left(3 - \frac{a}{2}\right)$ e as parcelas desta última soma pertencem respectivamente a $\varrho(2)$ e $\varrho(3)$, então $z \in \varrho(2) + \varrho(3)$.

445. Se α é um corte e $r > 0$ é um número racional, prove que $\alpha < \beta = \{a + r \mid a \in \alpha\}$.

446. Sejam $r, s \in \mathbb{Q}$ tais que $r < s$. Mostre que $\alpha = r + \frac{s - r}{\sqrt{2}}$ é irracional e que $r < \alpha < s$. Conclua daí que I é denso em $\mathbb{R}$.

Resolução: Se α fosse racional, então $\sqrt{2} = \frac{s - r}{\alpha - r}$ também o seria, o que é absurdo. Por outro lado, como $\sqrt{2} > 1$, então $0 < \frac{1}{\sqrt{2}} < 1$; daí $0 < \frac{s - r}{\sqrt{2}} < s - r$ e portanto $r < r + \frac{s - r}{\sqrt{2}} < s$.

447. Para quaisquer $a, b \in \mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geqslant 0\}$, prove que:

a) $0 \leqslant a \leqslant b \Rightarrow \sqrt{a} \leqslant \sqrt{b}$

b) $\sqrt{a + b} \leqslant \sqrt{a} + \sqrt{b}$

448. Para quaisquer $a, b \in \mathbb{R}$, prove que $2|ab| \leqslant a^2 + b^2$.

449. Prove por indução os seguintes resultados:

a) Para todo $a \in \mathbb{R}$, $0 < a < 1$, $(1 + a)^n < 1 + 2^n \cdot a$ $(\forall n \geqslant 1)$.

b) Se $a_1, a_2, \ldots, a_n$ $(n > 1)$ são números reais positivos $(a_i \geqslant 0$, $i = 1, 2, \ldots, n)$, então

$$(1 + a_1)(1 + a_2)\ldots(1 + a_n) \geqslant 1 + (a_1 + a_2 + \ldots + a_n)$$

450. Prove que, para todo $k \in \mathbb{R}$ e para todo número real $a > 1$, existe $n \in \mathbb{N}^*$ de modo que $a^n > k$.

451. Se a, b, c e d são números reais, prove que:

$$\sup\{a + c, b + d\} \leqslant \sup\{a, b\} + \sup\{c, d\}.$$

452. Seja A um subconjunto não vazio de $\mathbb{R}$. Um elemento $k \in \mathbb{R}$ se diz *cota inferior* de A se $k \leqslant x$, para todo $x \in A$. Um subconjunto $A \subset \mathbb{R}$, $A \neq \varnothing$, se diz *limitado inferiormente* se admite cotas inferiores em $\mathbb{R}$.

Se $A \neq \varnothing$ é um subconjunto de $\mathbb{R}$ limitado inferiormente, prove que o conjunto das cotas inferiores de A tem máximo, ou seja, que existe uma cota inferior que é maior que todas as outras, diferentes dela mesma. (O máximo das cotas inferiores é chamado *ínfimo* de A e é indicado por inf A.)

Sugestão: Mostre que $-A = \{-x \mid x \in A\}$ é limitado superiormente e que se s indica o supremo de A, então $-s = \inf A$.

453. Se $a, b \in \mathbb{R}$, mostre que

$$\sup\{a, b\} = \frac{a + b + |a - b|}{2} \quad \text{e} \quad \inf\{a, b\} = \frac{a + b - |a - b|}{2}$$

454. a) Seja $H \subset \mathbb{R}$ um subconjunto não vazio limitado superiormente. Prove que um certo $b \in \mathbb{R}$ é o supremo de H se, e somente se, dado $\varepsilon > 0$, $\varepsilon \in \mathbb{R}$, as seguintes condições se verificam: i $x < b + \varepsilon$, para todo $x \in H$; ii $x > b - \varepsilon$, para pelo menos um $x \in H$.

b) Enuncie e demonstre uma caracterização semelhante para $a = \inf H$, onde $H \neq \varnothing$ é um subconjunto de $\mathbb{R}$, limitado inferiormente.

455. Sejam A e B subconjuntos não vazios, e limitados inferiormente, de $\mathbb{R}$. Definindo $A + B = \{x + y \mid x \in A, y \in B\}$, prove que:

$$\inf(A + B) = \inf A + \inf B$$

Resolução: Se k_1 é uma cota inferior de A e k_2 é cota inferior de B, é claro que $k_1 + k_2$ é cota inferior de A + B e portanto este último conjunto é limitado inferiormente.

Como $\inf A \leqslant x$, $\forall x \in A$, e $\inf B \leqslant y$, $\forall y \in B$, então $\inf A + \inf B \leqslant x + y$, $\forall x \in A$ e $\forall y \in B$. Logo $\inf A + \inf B$ é cota inferior de $A + B$ e então $\inf A + \inf B \leqslant \inf(A + B)$. Por outro lado, para cada $x \in A$ fixado, vale a relação $\inf(A + B) - x \leqslant y$, $\forall y \in B$. Portanto $\inf(A + B) - x \leqslant \inf B$ ou $\inf(A + B) - \inf B \leqslant x$, para todo $x \in A$. Logo $\inf(A + B) - \inf B \leqslant \inf A$ ou, o que é equivalente, $\inf(A + B) \leqslant \inf A + \inf B$.

456. Sejam A e B subconjuntos de $\mathbb{R}$, não vazios e limitados superiormente. Prove que:

$$\sup (A + B) = \sup A + \sup B$$

457. Sejam A e B subconjuntos não vazios de $\mathbb{R}$. Se esses subconjuntos são limitados superiormente (respect., inferiormente) prove que:

$$\sup (A \cup B) = \sup\{\sup A, \sup B\}$$

$$(\text{respectivamente, } \inf(A \cup B) = \inf\{\inf A, \inf B\}).$$

458. Para todo $A \subset \mathbb{R}$, $A \neq \varnothing$, e para todo $c \in \mathbb{R}$, ponhamos, por definição, $cA = \{cx \mid x \in A\}$. Isso posto, se A é limitado ($\iff$ limitado superior e inferiormente), prove que:

a) $\sup (cA) = c \sup A$ se $c \geqslant 0$ e $\sup (cA) = c \inf A$ se $c \leqslant 0$

b) $\inf (cA) = c \inf A$ se $c \geqslant 0$ e $\inf (cA) = c \sup A$ se $c \leqslant 0$

459. Sejam A e B subconjuntos não vazios de $\mathbb{R}$, limitados inferiormente (respect., superiormente). Se $A \subset B$, prove que $\inf A \geqslant \inf B$ (respect. $\sup A \leqslant \sup B$).

Resolução (primeira parte): Por definição $\inf B \leqslant x$, $\forall x \in B$. Logo, $\inf B \leqslant x$, $\forall x \in A$, ou seja, $\inf B$ é uma cota inferior de A. Logo, $\inf B \leqslant \inf A$.

460. Seja $\varphi: \mathbb{R} \to \mathbb{R}$ um automorfismo (ver exercício 389).

a) Mostre que $\varphi(a) = a$, para todo $a \in \mathbb{Q}$.

b) Mostre que, para quaisquer $a, b \in \mathbb{R}$, $a < b \Rightarrow \varphi(a) < \varphi(b)$.

c) Se $\alpha \in I = \mathbb{R} - \mathbb{Q}$, prove que, também, $\varphi(\alpha) = \alpha$. (Logo, o único automorfismo de $\mathbb{R}$ é a aplicação idêntica.)

Sugestão para a): Ver resolução do exercício citado no enunciado.

Sugestão para b): $a < b \Rightarrow b - a = x^2$, para algum $x \in \mathbb{R}$; observar que $\varphi(x^2) = \varphi(x)^2 > 0$.

Resolução de c): Vamos supor, por exemplo, $\varphi(\alpha) < \alpha$ e tomemos $r \in \mathbb{Q}$ de maneira que $\varphi(\alpha) < r < \alpha$. De $r < \alpha$ segue que $\varphi(r) < \varphi(\alpha)$ (devido a b)); mas $\varphi(r) = r$, por a); assim $r < \varphi(\alpha) < r$, o que é absurdo.

461. Sejam A e B subconjuntos de $\mathbb{R}$ com a seguinte propriedade: $\sup A < \inf B$. Prove que $A \cap B = \varnothing$.

462. Mostre que, para todo inteiro $n > 1$, vale a relação:

$$\left(1 + \frac{1}{n+1}\right)^{n+1} > \left(1 + \frac{1}{n}\right)^n$$

Sugestão: Usar a desigualdade de Bernoulli para $a = -\dfrac{1}{(n+1)^2}$ e expoente do primeiro membro igual a $n + 1$.

4. A representação geométrica de $\mathbb{R}$

Mostraremos agora como, mediante algumas convenções, se pode estabelecer uma correspondência biunívoca entre os pontos de uma reta orientada (reta à qual se atribui um sentido positivo) e os elementos de $\mathbb{R}$. Em suma, vamos exibir um procedimento através do qual a cada ponto de uma reta orientada se pode associar um único número real de maneira que: a) a pontos diferentes correspondem números diferentes e, além disso, se um ponto X dessa reta está "à esquerda" de um ponto Y da mesma, então o número associado a X é menor que o associado a Y; b) Se $\alpha \in \mathbb{R}$, então há um único ponto da reta ao qual corresponde α. O número associado ao ponto chama-se *abscissa* desse ponto.

Mas isso pressupõe, evidentemente, os axiomas da geometria euclidiana, entre os quais o da *continuidade*, cujo enunciado é o seguinte: "Se os pontos de uma reta r são distribuídos em duas classes A e B tais que $A \cup B = r$ e todo ponto de A precede todo ponto de B, então existe em r um único ponto que não precede nenhum elemento de A e não segue nenhum de B".

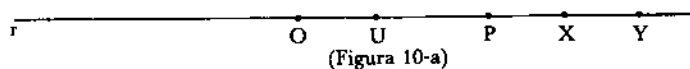
Isso posto consideremos uma reta orientada r. Sobre r fixam-se dois pontos distintos O e U de modo que o segmento orientado OU tenha sentido concorde com o sentido positivo de r (que suporemos, como é praxe, da esquerda para a direita). Os pontos O e U são chamados, respectivamente, *ponto origem* e *ponto unidade* de r (fig. 10-a).

Ao ponto O atribui-se como abscissa o número 0. Seja $P \in r$ um ponto à direita de O. Há duas possibilidades:

i Os segmentos de reta OP e OU são comensuráveis. Quando isto acontece existe um número racional $a > 0$ tal que a medida de OP, tomando como unidade $u = OU$, é a. Ou seja:

$$\overline{OP} = a$$

Nesse caso a abscissa de P é, por definição, o número racional a.

(Figura 10-a)

Convém notar, por outro lado, que, conforme já mostramos no item 1, dado um número racional $a > 0$, existe P na semi-reta $\overrightarrow{OU}$ de maneira que a medida de OP em relação a $u = OU$ é a. Logo, a abscissa de P é a e pode-se dizer que $\overrightarrow{OU}$ contém todos os pontos de abscissas racionais positivas.

Antes de passarmos à outra possibilidade, enunciaremos (e justificaremos) algumas observações necessárias ao que vem a seguir:

- Se X e Y são pontos quaisquer de r, à direita de O (o primeiro poderia ser o próprio O), $X \neq Y$, então entre X e Y há um ponto de abscissa racional.

Justificativa: Imaginemos X e Y como na figura 10-a e tomemos $r \in \mathbb{N}^*$ de maneira que $\frac{1}{r} \cdot OU < XY$. Seja s o menor número natural que verifica a relação:

$$s \cdot \left(\frac{1}{r} \cdot OU\right) = \frac{s}{r} \cdot OU > OX$$

Isso mostra que o ponto de abscissa $\frac{s}{r}$ está à direita de X. Mas como

$$\frac{s}{r} \cdot OU = \frac{s-1}{r} \cdot OU + \frac{1}{r} \cdot OU < OX + XY = OY$$

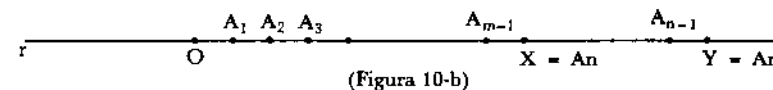
concluímos que esse mesmo ponto está à esquerda de Y. Logo, está entre X e Y.

- "Se X e Y são pontos de r de abscissas racionais situados à direita de O e X precede Y, então a abscissa de X é menor que a de Y."

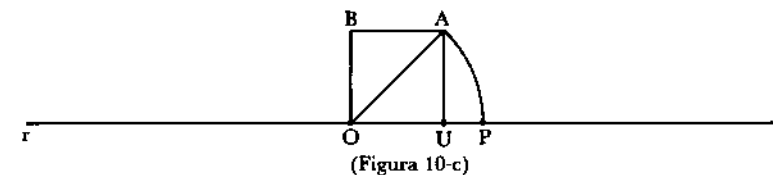
Justificativa: Podemos supor essas abscissas iguais, respectivamente, a $\frac{m}{r}$ e $\frac{n}{r}$. Como, então, m indica o número de pontos $A_1, A_2, \ldots, A_m = X$ de OX tais que $OA_1, A_1A_2, \ldots, A_{m-1}X$, são todos congruentes a $\frac{1}{r} \cdot OU$ (fig. 10-b) e n indica o número de pontos $A_1, A_2, \ldots, A_n = Y$ de OY para os quais, também, $OA_1, A_1A_2, \ldots, A_{n-1}Y$ são todos congruentes a $\frac{1}{r} \cdot OU$, pode-se

concluir que $m < n$ e daí que $\frac{m}{r} < \frac{n}{r}$.

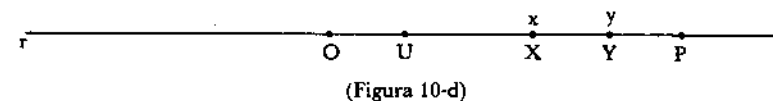
A_1 A_2 A_3 A_{m-1} A_{n-1}
r O X = An Y = An

(Figura 10-b)

- "Numa reta orientada r, de ponto origem O e ponto unidade U, existem pontos P, à direita de O, tais que OP e OU são incomensuráveis."

Justificativa: Consideremos o quadrado OUAB (fig. 10-c). Se P é a intersecção da circunferência de raio OA com r, então OP — por ser congruente a OA — é incomensurável com OU (ver item 1).

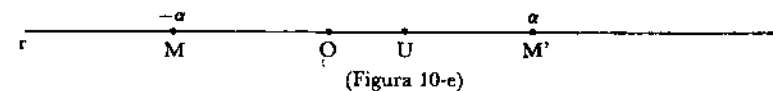
(Figura 10-c)

ii Os segmentos OP e OU são incomensuráveis. Para esta hipótese, consideremos o conjunto $\alpha \subset \mathbb{Q}$ assim definido: $x \in \alpha \iff x < 0$ ou ($x \geqslant 0$ e x é abscissa de algum ponto à esquerda de P). Pode-se provar que tal conjunto é um corte em $\mathbb{Q}$. Por brevidade vamos nos ater à última condição do conceito de corte (definição 1).

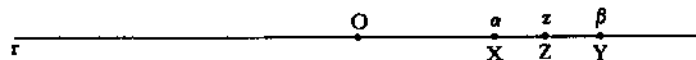
Seja $x \in \alpha$, digamos $x > 0$. Então x é a abscissa de algum ponto X de r, à esquerda de P (fig. 10-d). Consideremos a seguir um ponto Y, entre X e P, de abscissa racional y.

(Figura 10-d)

Então $y \in \alpha$ (pois $y \in \mathbb{Q}$ e y está à esquerda de P) e $y > x$ (devido à segunda observação feita em **i**). Logo há um número racional em α maior que x, o que prova a condição referida.

Sendo α um corte em $\mathbb{Q}$, então $\alpha \in \mathbb{R}$. O número α é, por definição, a abscissa de P.

Consideremos agora um ponto M à esquerda de O e seja M' seu simétrico em relação a O. Se a abscissa de M' é α (fig. 10-e), então a de M é, por definição, $-\alpha$.

(Figura 10-e)

Portanto, a cada ponto de uma reta orientada r fica associado, conforme procedimento exposto, um único número real. Mostremos que, sem exceção, nessa correspondência, se X está à esquerda de Y, então a abscissa α de X é menor que a abscissa β de Y.

De fato, suponhamos que $\beta \leqslant \alpha$ e tomemos entre X e Y um ponto Z de abscissa racional z (fig. 10-f).

(Figura 10-f)

Mostremos primeiro que, considerando β como um corte em $\mathbb{Q}$, então $z \in \beta$. De fato, se $\beta \in \mathbb{Q}$, como Z está à esquerda de Y, então $z < \beta$ (conforme observação feita em i) e daí $z \in \beta$; se $\beta \notin \mathbb{Q}$, então a própria definição de abscissa neste caso garante que $z \in \beta$. Levando em conta, porém, que estamos supondo $\beta \subset \alpha$ ($\iff \beta \leqslant \alpha$), então $z \in \alpha$, o que é absurdo. Donde, efetivamente, $\alpha < \beta$.

Em particular a correspondência

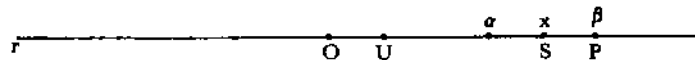
$$\text{Pontos de r} \rightarrow \text{Números reais}$$

que acabamos de estabelecer, é injetora. Ou seja, a pontos diferentes da reta orientada, correspondem números reais diferentes.

Mostremos que é também sobrejetora. Quer dizer, nessa correspondência não "sobram" números reais. Para tanto podemos restringir nosso raciocínio aos números reais $\alpha > 0$.

Se $\alpha \in \mathbb{Q}$, já vimos no item 1 como obter em r um ponto, à direita de O, de maneira que $\overline{OP} = \alpha$. Como a abscissa de P é α, então a P corresponde α.

Se $\alpha \notin \mathbb{Q}$, dividamos os pontos de r em duas classes A e B, assim definidas: em A ficam todos os pontos de abscissa menor que α; em B todos os pontos de abscissa maior que ou igual a α. Se L e M são pontos de A e B de abscissas x e y, respectivamente, então $x < \alpha \leqslant y$ e daí $x < y$. Logo L precede M. Assim, A e B satisfazem as condições do axioma da continuidade — e, portanto, fica determinado em r um único ponto P que não precede nenhum elemento de A e não segue nenhum de B.

Seja β a abscissa de P e mostremos que $\beta = \alpha$, o que encerra a justificativa. Vamos supor $\beta > \alpha$ e tomemos $x \in \mathbb{Q}$, $\alpha < x < \beta$. Se S é o ponto de abscissa x (fig. 11), então $S \in B$ (pois $x > \alpha$). Mas como $x < \beta$, então P segue S. Absurdo, pois P não segue nenhum ponto de B. Igualmente não pode ocorrer $\beta < \alpha$. Donde $\beta = \alpha$ e ao ponto P corresponde α.

(Figura 11)

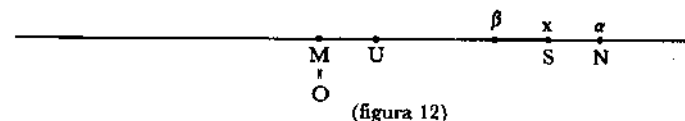
A correspondência considerada estabelece sobre a reta orientada r o que se chama de *sistema de abscissas*, cujos elementos fundamentais são o ponto origem O e o ponto unidade U.

4.1 Medida de um segmento de reta incomensurável com a unidade

No item 1 tratamos do conceito de medida de um segmento de reta, no caso de este ser comensurável com a unidade de comprimento. Nesse caso a medida é sempre um número racional positivo.

Seja agora MN um segmento de reta incomensurável com a unidade escolhida. Consideremos a reta orientada pelos pontos M e N, com sentido positivo de M para N, e ponhamos sua origem em M. Seja U o ponto de r, à direita de M, tal que MU é congruente com u. Nessas condições, se a abscissa de N é o número irracional α, então se diz que a *medida* de MN é α e escreve-se:

$$\overline{MN} = \alpha$$

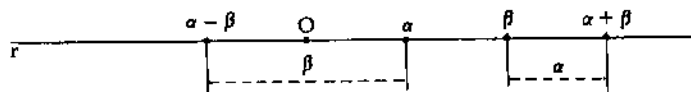
(naturalmente medida em relação a u).

(figura 12)

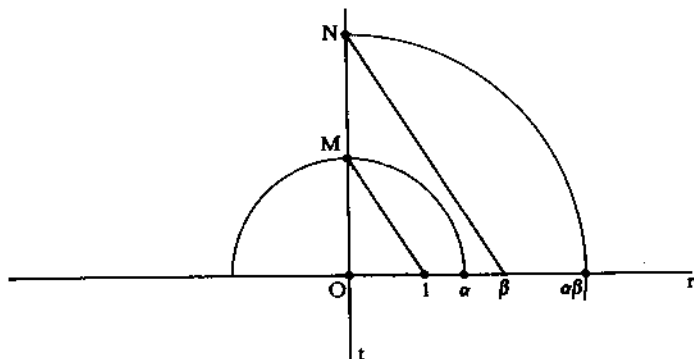
Em resumo, α é o corte em $\mathbb{Q}$ formado pelas abscissas de todos os pontos racionais à esquerda de N. Então α inclui todas as aproximações racionais por falta $\frac{r}{s}$ da medida de MN, para as quais vale:

$$0 < \frac{r}{s} < \alpha$$

Na verdade, como provaremos a seguir, α é o supremo do conjunto dessas aproximações. E imediato primeiro que α é uma cota superior desse conjunto. Provemos que é a menor delas. Suponhamos que um número real $\beta < \alpha$ também fosse cota superior desse conjunto e tomemos $x \in \mathbb{Q}$, $\beta < x < \alpha$ (fig. 12). Se S é o ponto de r de abscissa x, então $x = \overline{OS}$ é uma aproximação racional por falta da medida de MN. Mas isso é absurdo pois $x > \beta$.

Exemplo 13: Se α e β são abscissas de pontos de uma reta orientada r, vejamos como construir, apenas com régua (sem escala) e compasso, os pontos dessa reta de abscissas $\alpha \pm \beta$, $\alpha\beta$, α^{-1} (quando $\alpha \neq 0$) e $\sqrt{\alpha}$ (quando $\alpha > 0$).

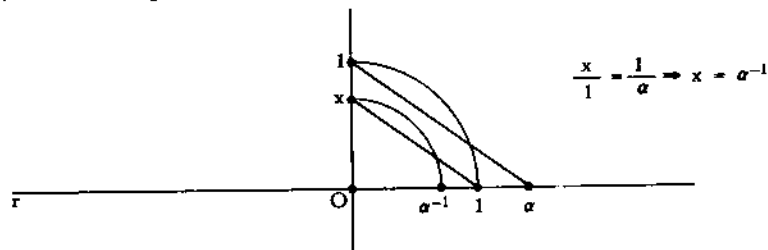
A construção de $\alpha \pm \beta$ é imediata (ver fig. 13).

(Figura 13)

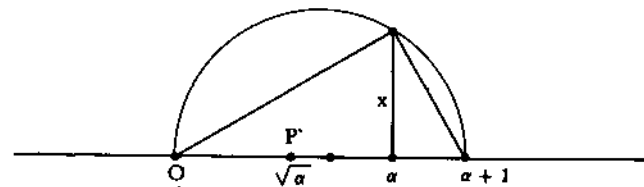
Para construirmos o ponto de abscissa $\alpha\beta$, traçamos à perpendicular a r pelo ponto origem, o que pode ser feito com régua e compasso. Seja t essa perpendicular. Se M é uma das intersecções de t com a circunferência de centro na origem e raio α, então OM = α. Traçamos o segmento de reta que liga M ao ponto de abscissa 1 e, a seguir, a paralela por β a esse segmento (fig. 14).

(Figura 14)

Se N é a intersecção dessa paralela com t, o teorema de Tales garante que:

$$\frac{\overline{ON}}{\overline{OM}} = \frac{\beta}{1}$$

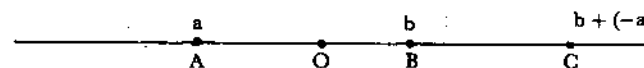
Mas $\overline{OM} = \alpha$ e portanto $\overline{ON} = \alpha\beta$. Assim, a intersecção da circunferência de centro O e raio ON com r, à direita de O, é o ponto procurado (pois trabalhamos com $\alpha > 0$ e $\beta > 0$).

A construção de α^{-1} ($\alpha \neq 0$) se faz conforme o procedimento fixado na figura 15, onde a reta por 1 e x é paralela à reta por α e 1.

(Figura 15)

Para a construção de $\sqrt{\alpha}$ ($\alpha > 0$) marcamos sobre r o ponto de abscissa $\alpha + 1$ (além do ponto α, dado). Traçamos a semicircunferência da qual o segmento de extremidades na origem e no ponto $\alpha + 1$ é diâmetro (fig. 16). Pelo ponto de abscissa α levantamos o segmento perpendicular a r, até alcançar a semicircunferência. Se x é a medida desse segmento, $x = \sqrt{\alpha \cdot 1} = \sqrt{\alpha}$. O ponto P tal que $\overline{OP} = x$ é o ponto procurado.

(Figura 16)

4.2 Distância entre pontos

Consideremos uma reta orientada r, de origem O, munida de um sistema de abscissas. Dados A, B ∈ r (fig. 17), chamamos de *distância entre* A e B e indicamos por d(A, B) a medida do segmento AB. Ou seja

$$d(A, B) = \overline{AB}$$

(Figura 17)

A medida de AB é, por definição, a abscissa do ponto C, à direita de O, tal que OC é congruente com AB.

Examinemos o caso mostrado na figura 17. Se a abscissa de A é a e a de B é b, então a de C é $b + (-a) = b - a = |a - b|$, pois $b - a > 0$. Assim:

$$d(A, B) = |a - b|$$

A aplicação desse raciocínio a todas as situações possíveis leva sempre ao mesmo resultado: "a distância entre dois pontos quaisquer de uma reta orientada munida de um sistema de abscissas é igual ao valor absoluto da diferença entre suas abscissas".

Assim, por exemplo, quando se escreve $|x - a| < \varepsilon$ ou $|a_n - a| < \varepsilon$, isso significa que a distância entre o ponto x (ou seja, ponto de abscissa x) e o ponto a, ou entre o ponto a_n e o ponto a, é menor que ε.

Podemos encarar d como uma função de r × r em IR. Para essa função valem as seguintes propriedades:

- $d(A, B) \geqslant 0$; $d(A, B) = 0 \iff A = B$
- $d(A, B) = d(B, A)$
- $d(A, B) \leqslant d(A, C) + d(C, B)$

A demonstração da última, supondo que A, B e C tenham abscissas respectivamente iguais a a, b e c, se faz assim:

$$d(A, B) = |a - b| = |a - c + c - b| \leqslant |a - c| + |c - b| = d(A, C) + d(C, B).$$

EXERCÍCIOS

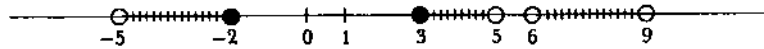
463. Construir geometricamente, com régua e compasso, os pontos de abscissas $\sqrt{3}$, $\sqrt{2} + \sqrt{3}$ e $\sqrt{5} - \sqrt{3}$.

464. a) Se a abscissa de um ponto é dada por cos α, construa geometricamente o ponto de abscissa sen α.
b) E dado o ponto de abscissa sen α, construa o ponto de abscissa cos α.

465. Dados $a, b \in \mathbb{R}$, $a < b$, o *intervalo* de extremos a e b, fechado em ambos os extremos, é o seguinte subconjunto de $\mathbb{R}$:

$$[a, b] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$$

De maneira óbvia se definem $[a, b[= \{x \in \mathbb{R} \mid a \leqslant x < b\}$, $]a, b]$ e $]a, b[$. Na figura destacamos os intervalos $]-5, -2]$, $[3, 5[$ e $]6, 9[$.

−5 −2 0 1 3 5 6 9

Mostrar que $]0, 1[$ tem a mesma *cardinalidade* de $[0, 1]$. (Dois conjuntos não vazios têm a *mesma cardinalidade* se é possível definir $f : A \to B$, f bijetora.)

Resolução: Observemos que $[0, 1] = A \cup \left\{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$ e que $]0, 1[= A \cup \left\{\frac{1}{2}, \frac{1}{3}, \ldots\right\}$, onde $A = [0, 1] - \left\{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$. (Ou $A =]0, 1[- \left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$.) A função $f : [0, 1] \to]0, 1[$ definida por

$$\begin{array}{ccccccc} \{0, & 1, & \frac{1}{2}, & \frac{1}{3}, & \ldots\} & \cup & A \\ \downarrow & \downarrow & \downarrow & \downarrow & & & \downarrow \\ \{\frac{1}{2}, & \frac{1}{3}, & \frac{1}{4}, & \frac{1}{5}, & \ldots\} & \cup & A \end{array} \quad \text{(identidade)}$$

ou seja, a função dada por

$$f(x) = \begin{cases} \frac{1}{2} \text{ se } x = 0 \\ \frac{1}{n+2} \text{ se } x = \frac{1}{n} \\ x \text{ se } x \in A \end{cases}$$

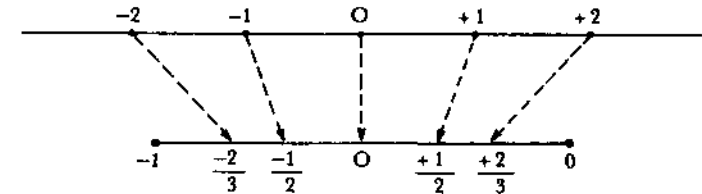
é bijetora (justifique). Logo, efetivamente, $[0, 1]$ e $]0, 1[$ têm mesma cardinalidade.

466. Mostre que $[0, 1[$ e $]0, 1]$ têm mesma cardinalidade que $[0, 1]$.

467. Para quaisquer $a, b \in \mathbb{R}$, $a < b$, prove que os intervalos $[a, b]$, $[a, b[$, $]a, b]$ e $]a, b[$ têm mesma cardinalidade que $[0, 1]$.

Sugestão: Mostre que, por exemplo, $[a, b]$ e $[0, 1]$ têm mesma cardinalidade, provando que $f(x) = a + (b - a)\,x$ define uma função bijetora de $[0, 1]$ em $[a, b]$. Analogamente $[0, 1[$ tem mesma cardinalidade que $[a, b[$, etc. Usar os dois exercícios anteriores.

Nota: Pelo exercício anterior, todo intervalo $[a, b]$, não importa quão grande seja sua amplitude, tem a mesma cardinalidade de $[0, 1]$. Isso significa, intuitivamente, que $[a, b]$ e $[0, 1]$ têm a "mesma quantidade" de pontos, $\forall a, b \in \mathbb{R}$, $a < b$. Por exemplo, a cardinalidade de $[-10^{1\,000}, 10^{1\,000}]$ é a mesma que a de $[0, 1]$.

468. Mostre que $f(x) = \frac{x}{1 + |x|}$ define uma função de $\mathbb{R}$ em $]-1, +1[$ e que esta função é bijetora. Que conclusão se pode tirar, a esta altura, em termos de cardinalidade, para os intervalos em $\mathbb{R}$?

5. Seqüência de números reais

Uma função $f : \mathbb{N}^* \to \mathbb{R}$ recebe o nome de *seqüência* de números reais. Se fizermos $f(n) = a_n$ ($n = 1, 2, 3, \ldots$), então a notação que se usa para indicar a seqüência f é $(a_1, a_2, \ldots, a_n, \ldots)$ ou, resumidamente, (a_n). As imagens

a_n são chamadas *termos* da seqüência. Obviamente a escolha da letra a para indicar os termos de uma seqüência genérica é arbitrária.

Exemplos:

$(a_n) = (1, 1, 1, \ldots)$

$(b_n) = (1, 2, 3, 3, 3, \ldots, 3, \ldots)$

$(c_n) = \left(1, \frac{1}{2}, \frac{1}{3}, \ldots\right)$

$(d_n) = \left(\sqrt{2}, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{3}, \ldots\right)$

Uma seqüência (a_n) se diz *estacionária* se existe um índice r de modo que $a_r = a_{r+1} = a_{r+2} = \ldots$. Uma seqüência estacionária (a_n) em que $a_1 = a_2 = \ldots = a_n = \ldots$ é chamada *constante*. Dos exemplos anteriores, as duas primeiras são estacionárias, sendo a primeira constante.

DEFINIÇÃO 3 Diz-se que uma seqüência de números reais (a_n) *converge* para um número $a \in \mathbb{R}$ se, dado $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, existe um índice r (que depende de ε) de maneira que:

$$|a_n - a| < \varepsilon, \text{ para todo } n \geqslant r$$

Nesse caso diz-se também que (a_n) é uma *seqüência convergente* em $\mathbb{Q}$ e que a é *limite* de (a_n). Usam-se as seguintes notações para exprimir que a é limite de (a_n):

$$\lim_{n\to\infty} a_n = a; \lim a_n = a; a_n \to a$$

PROPOSIÇÃO 3 (*unicidade do limite*): Uma seqüência (a_n) em $\mathbb{R}$ não pode convergir para mais do que um número real.

Demonstração: Seja (a_n) uma seqüência em $\mathbb{R}$ e suponhamos que existam $a, b \in \mathbb{R}$, $a \neq b$, de modo que $\lim a_n = a$ e $\lim a_n = b$. Pondo-se $2\varepsilon = |a - b|$, então $\varepsilon \in \mathbb{R}$ e $\varepsilon > 0$. Daí, levando em conta nossas suposições, temos garantida a existência de índices r_1 e r_2 tais que:

$$|a_n - a| < \varepsilon, \forall n \geqslant r_1$$
$$|a_n - b| < \varepsilon, \forall n \geqslant r_2$$

Assim, para todo $n \geqslant r_1$ e $n \geqslant r_2$, simultaneamente:

$$2\varepsilon = |a - b| = |a - a_n + a_n - b| \leqslant |a - a_n| + |a_n - b| < \varepsilon + \varepsilon = 2\varepsilon$$

o que é absurdo. ■

Exemplo 14: Uma seqüência estacionária $(a_1, a_2, \ldots, a_{r-1}, a, a, \ldots, a, \ldots)$ converge para a.

De fato, para todo $n \geqslant r$:

$$|a_n - a| = |a - a| = 0$$

Logo, dado $\varepsilon > 0$, para todo $n \geqslant r$:

$$|a_n - a| = 0 < \varepsilon$$

Em particular uma seqüência constante $(a, a, \ldots, a, \ldots)$ converge para a.

Exemplo 15: Mostremos que $\left(\frac{1}{n}\right) = \left(1, \frac{1}{2}, \frac{1}{3}, \ldots\right)$ converge para 0.

Como $\mathbb{R}$ é arquimediano, dado $\varepsilon > 0$, existe $r \in \mathbb{N}^*$ de maneira que:

$$r \cdot 1 = r > \varepsilon^{-1}$$

Portanto:

$$r^{-1} = \frac{1}{r} < \varepsilon$$

Como porém

$$n \geqslant r \Rightarrow \frac{1}{n} \leqslant \frac{1}{r}$$

então, para todo $n \geqslant r$:

$$\left|\frac{1}{n} - 0\right| = \left|\frac{1}{n}\right| = \frac{1}{n} \leqslant \frac{1}{r} < \varepsilon$$

Exemplo 16: Se uma seqüência (a_n) em $\mathbb{R}$ converge para o número real a, então, para todo $s \geqslant 0$, a seqüência (b_n), onde $b_1 = a_{s+1}$, $b_2 = a_{s+2}$, $b_3 = a_{s+3}$, ..., também converge para a.

Dado $\varepsilon > 0$, existe um índice r tal que $|a_n - a| < \varepsilon$, sempre que $n \geqslant r$. Logo, para todo $n \geqslant r$:

$$|b_n - a| = |a_{s+n} - a| < \varepsilon$$

pois $s + n \geqslant n \geqslant r$.

Como $\left(1, \frac{1}{2}, \frac{1}{3}, \ldots\right)$ converge para 0, então $\left(\frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \ldots\right)$, por exemplo, também converge para 0.

Exemplo 17: Se q é um número real situado no intervalo $0 < q < 1$, então a seqüência $(q^n) = (1, q, q^2, \ldots)$ converge para 0.

Seja $\varepsilon > 0$. Como $0 < q < 1$, o exemplo 11 nos garante que existe $r \in \mathbb{N}^*$ para o qual vale $q^r < \varepsilon$. Mas, de acordo com o exemplo 9: $m \geq n \Rightarrow$ $\Rightarrow q^m \leq q^n$. Logo, para todo $n \geq r$:

$$|q^n - 0| = q^n \leq q^r < \varepsilon$$

PROPOSIÇÃO 4 Se (a_n) é uma seqüência de números reais, convergente em $\mathbb{R}$, então existe $k \in \mathbb{R}$, $k > 0$, de tal sorte que $|a_n| < k$, para todo $n \geq 1$.

Demonstração: Tomando-se $\varepsilon = 1$ (por exemplo) e supondo $\lim a_n = a$, então existe um índice r tal que:

$$|a_n - a| < 1, \forall n \geq r$$

Como

$$|a_n| - |a| \leq |a_n - a|$$

então

$$|a_n| - |a| < 1$$

e portanto:

$$|a_n| < 1 + |a|, \forall n \geq r$$

Assim, se tomarmos k maior que cada um dos números

$$|a_1|, |a_2|, \ldots, |a_{r-1}|, 1 + |a|$$

então é evidente que:

$$|a_n| < k, \forall n \geq 1$$

■

Nota: Uma seqüência (a_n) em $\mathbb{R}$ se diz *limitada* se, para um conveniente $k \in \mathbb{R}$, $k > 0$, vale $|a_n| < k$, para todo $n \geq 1$. Logo, pelo que vimos, toda seqüência convergente é limitada. A recíproca não é verdadeira. De fato, considerando por exemplo a seqüência $(1, 2, 1, 2, 1, 2, \ldots) = (a_n)$, então $|a_n| < 3, \forall n \geq 1$, mas (a_n) não converge para nenhum $a \in \mathbb{R}$. Para justificar esta última afirmação tomemos $\varepsilon = \frac{1}{2}$. Admitindo que $a_n \to a$, então $|1 - a| = |a - 1| < \frac{1}{2}$; daí $\frac{1}{2} < a < \frac{3}{2}$; mas então $|2 - a| > \varepsilon = \frac{1}{2}$, o que não é possível.

DEFINIÇÃO 4 Sejam (a_n) e (b_n) seqüências de números reais. Por definição, a *soma* e o *produto* da primeira pela segunda são, respectivamente, $(a_n) + (b_n) = (a_n + b_n) = (a_1 + b_1, a_2 + b_2, \ldots)$ e $(a_n)(b_n) = (a_n b_n) =$ $= (a_1 b_1, a_2 b_2, \ldots)$, ambas obviamente também seqüências em $\mathbb{R}$. Se $c \in \mathbb{R}$, o *produto* de c por (a_n) é definido por $c(a_n) = (ca_n) = (ca_1, ca_2, \ldots)$.

Por exemplo, se $(a_n) = \left(1, \frac{1}{2}, \ldots \frac{1}{n}, \ldots\right)$; $(b_n) = \left(\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots, \frac{n}{n+1}, \ldots\right)$ e $c = 2$, então

$$(a_n + b_n) = \left(\frac{3}{2}, \frac{7}{6}, \frac{13}{12}, \ldots, \frac{n^2+n+1}{n(n+1)}, \ldots\right)$$

$$(a_n b_n) = \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots, \frac{1}{n+1}, \ldots\right)$$

$$2(a_n) = \left(2, 1, \frac{2}{3}, \ldots, \frac{2}{n}, \ldots\right)$$

PROPOSIÇÃO 5 Sejam (a_n) e (b_n) seqüências de números reais convergentes para a e b, respectivamente, e seja $c \in \mathbb{R}$. Então a soma e o produto de ambas, bem como o produto de qualquer uma por c, também convergem em $\mathbb{R}$ e:

$$\lim (a_n + b_n) = a + b, \ \lim (a_n b_n) = ab \ \text{e} \ \lim (ca_n) = ca$$

Demonstração: Faremos a prova apenas para o produto de (a_n) por (b_n). Seja k um número real tal que $k > |a_n|$, para todo índice n, e $k > |b|$. A existência de k é garantida pela proposição 4 e pelo fato de que sempre há um número real maior que dois outros dados.

Seja $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$. Como $a_n \to a$ e $b_n \to b$, considerando o número real $\frac{\varepsilon}{2k} > 0$, existem índices r_1 e r_2 tais que:

$$|a_n - a| < \frac{\varepsilon}{2k}, \forall n \geq r_1$$

$$|b_n - b| < \frac{\varepsilon}{2k}, \forall n \geq r_2$$

Logo, para todo n maior que r_1 e r_2:

$$|a_n b_n - ab| = |a_n b_n - a_n b + a_n b - ab| \leq |a_n b_n - a_n b| + |a_n b - ab| =$$

$$= |a_n||b_n - b| + |b||a_n - a| < k \frac{\varepsilon}{2k} + k \frac{\varepsilon}{2k} = \varepsilon$$

o que prova que $a_n b_n \to ab$. ■

Por exemplo, como $(a_n) = \left(\frac{1}{n}\right)$ converge para 0 e $(b_n) = \left(\frac{n}{n+1}\right)$ converge para 1, então $(a_n + b_n) = \frac{n^2+n+1}{n(n+1)}$ converge para 1, $(a_n b_n) = \left(\frac{1}{n+1}\right)$ converge para 0 e $2(b_n) = \left(\frac{2n}{n+1}\right)$ converge para 2.

DEFINIÇÃO 5 Uma seqüência (a_n) se diz *crescente* se $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n \leqslant a_{n+1} \leqslant \ldots$. E se $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant a_{n+1} \geqslant \ldots$, então (a_n) é chamada seqüência *decrescente*.

Por exemplo, $(1, 1, 2, 2, 3, 3, \ldots, n, n, n+1, n+1, \ldots)$ é crescente; $\left(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots\right)$ é um exemplo de seqüência decrescente.

PROPOSIÇÃO 6 Seja (a_n) uma seqüência crescente de números reais. Se essa seqüência é limitada e se $a = \sup \{a_n | n \geqslant 1\}$, então $\lim a_n = a$.

Demonstração: Como (a_n) é limitada, então existe $k \in \mathbb{R}$ de modo que $|a_n| < k$, $\forall n \geqslant 1$. Como $a_n \leqslant |a_n| < k$, para todo $n \geqslant 1$, então $\{a_n | n \geqslant 1\}$ é limitado superiormente e portanto admite supremo $a \in \mathbb{R}$. Dado $\varepsilon > 0$, como $a - \varepsilon < a$, então existe um índice r tal que $a - \varepsilon < a_r \leqslant a$. De fato, se $a_n \leqslant a - \varepsilon$ para todo $n \geqslant 1$, então $a - \varepsilon$ seria uma cota superior de $\{a_n | n \geqslant 1\}$ menor que a, o que não é possível.

Mas então

$$a - \varepsilon < a_r \leqslant a_{r+1} \leqslant \ldots \leqslant a < a + \varepsilon$$

ou seja:

$$a - \varepsilon < a_n < a + \varepsilon, \forall n \geqslant r$$

Mas isso implica que (segundo vimos em 3):

$$|a_n - a| < \varepsilon, \forall n \geqslant r$$

Donde $\lim a_n = a$. ■

EXERCÍCIOS

469. Mostre que:

a) $\lim \frac{n}{n+1} = 1$

b) $\lim \frac{1}{\sqrt{n}} = 0$

c) $\lim \left(\frac{2^{n+1} + 3^{n+1}}{2^n + 3^n}\right) = 3$

d) $\lim \left(\frac{1}{n^2} + \frac{2}{n^2} + \ldots + \frac{n-1}{n^2}\right) = \frac{1}{2}$

470. Dada uma seqüência (a_n) em $\mathbb{R}$, se $\{r_1, r_2, r_3, \ldots\} \subset \mathbb{N}^*$ e $r_1 < r_2 < r_3 < \ldots$, então $(b_1, b_2, b_3, \ldots) = (a_{r_1}, a_{r_2}, a_{r_3}, \ldots)$ chama-se subseqüência de (a_n).

a) Se $a_n \to a$, prove que toda subseqüência de (a_n) também converge para a.

b) Dê exemplos de seqüências que admitem subseqüências convergentes mas que elas próprias não convergem.

c) Seja (a_n) uma seqüência em $\mathbb{R}$. Se as subseqüências $(a_1, a_3, a_5, \ldots)$ e $(a_2, a_4, a_6, \ldots)$ convergem para a, mostre que $\lim a_n = a$.

Resolução de c): Dado $\varepsilon > 0$, existem por hipótese índices r_1 (ímpar) e r_2 (par) de maneira que $|a_n - a| < \varepsilon$ para todo índice ímpar $n \geqslant r_1$ e para todo índice par $n \geqslant r_2$. Se $r = \max\{r_1, r_2\}$, então $|a_n - a| < \varepsilon$, para todo $n \geqslant r$, o que conclui a justificativa.

471. Seja (a_n) uma seqüência em $\mathbb{R}$. Se as subseqüências (a_{2n}), (a_{2n+1}) e (a_{3n+1}) convergem para a, b e c, prove que $a = b = c$ e que (a_n) converge também para esse valor comum.

472. Se $\lim a_n = a$, prove que $\lim |a_n| = |a|$.

473. Prove que: $\lim a_n = a \iff \lim |a_n - a| = 0$.

474. Considere a seqüência de números racionais definida por recorrência da seguinte maneira:

$$a_1 = 2 \quad \text{e} \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right) \quad (n \geqslant 1)$$

Mostrar que (a_n) é decrescente (estritamente, ou seja, $a_1 > a_2 > a_3 > \ldots$) e que $a_n > 1$, para todo $n \geqslant 1$.

Resolução: Como $a_n - \frac{2}{a_n} \neq 0$, pois cada a_n é racional, e como

$$a_{n+1}^2 = \frac{1}{4}\left(a_n + \frac{2}{a_n}\right)^2 = \frac{1}{4}\left(a_n - \frac{2}{a_n}\right)^2 + 2$$

então $a_n^2 > 2$, para todo $n \geqslant 1$. Daí

$$a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right) < \frac{1}{2}\left(a_n + \frac{a_n^2}{a_n}\right) = a_n$$

para todo $n \geqslant 1$. Logo, $a_1 > a_2 > a_3 > \ldots$ e (a_n) é estritamente decrescente. Vamos supor

$$a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right) \leqslant 1$$

Então $a_n^2 - 2a_n + 2 \leqslant 0$, o que é impossível pois $\Delta < 0$.

475. Seja (a_n) uma seqüência decrescente e limitada. Mostre que $A = \{a_n | n \geqslant 1\}$ é limitado inferiormente e que se $a = \inf A$, então (a_n) converge para a.

Sugestão: Exercício 452 e proposição 6.

476. i Classifique em crescente ou decrescente (se for o caso) cada uma das seguintes seqüências:

a) $\left(\dfrac{3n-1}{4n+5}\right)$ d) $(\text{sen}\,(n\pi))$

b) $\left(\dfrac{5^n}{1+5^{2n}}\right)$ e) $\left(\dfrac{n}{2^n}\right)$

c) $(n^2 + (-1)^n n)$ f) $\left(\dfrac{n+1}{n+2}\right)$

ii Das seqüências crescentes ou decrescentes, quais as que são limitadas?

iii Determine o limite destas últimas.

477. Mostre que a seqüência do exercício 474 converge em $\mathbb{R}$ e que seu limite é $\sqrt{2}$.

Sugestão: Exemplo 16 e proposição 5.

478. a) Sejam (a_n) e (b_n) seqüências de números reais convergentes respectivamente para $a \in \mathbb{R}$ e $b \in \mathbb{R}$. Se $a_n \geqslant b_n$, a partir de um certo índice, mostre que $a \geqslant b$.

b) Sejam (a_n), (b_n) e (c_n) seqüências em $\mathbb{R}$ tais que, a partir de algum índice, $a_n \leqslant b_n \leqslant c_n$. Se $\lim a_n = \lim c_n = a \in \mathbb{R}$, prove que (b_n) também converge para a.

Resolução de b): Seja r_o o índice a partir do qual $a_n \leqslant b_n \leqslant c_n$. Assim, para todo $n \geqslant r_o$, $-a_n \geqslant -b_n \geqslant -c_n$ e portanto: $a - a_n \geqslant a - b_n \geqslant$ $\geqslant a - c_n$. Por hipótese existe r_1 tal que $|a - a_n| < \varepsilon$, $\forall n \geqslant r_1$, e existe r_2 tal que $|a - c_n| < \varepsilon$, $\forall n \geqslant r_2$. Seja $r = \max\{r_o, r_1, r_2\}$. Para todo $n \geqslant r$ há duas possibilidades: i $a - b_n \geqslant 0$, o que implica $a - a_n \geqslant 0$ e então $|a - b_n| \leqslant |a - a_n| < \varepsilon$. ii $a - b_n \leqslant 0$, do que segue $b_n - a \geqslant 0$ e então $|b_n - a| \leqslant |c_n - a| < \varepsilon$. Portanto $|b_n - a| < \varepsilon$, $\forall n \geqslant r$, o que implica $a = \lim b_n$.

6. Séries infinitas de números reais

DEFINIÇÃO 6 Seja (a_n) uma seqüência em $\mathbb{R}$. Indicaremos por

$$a_1 + a_2 + \ldots + a_n + \ldots$$

ou, abreviadamente, por

$$\sum_{i=1}^{\infty} a_i$$

e chamaremos *série* determinada por (a_n) a seqüência (s_n), onde:

$$s_1 = a_1$$
$$s_2 = a_1 + a_2$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$s_n = a_1 + a_2 + \ldots + a_n$$
$$\ldots\ldots\ldots\ldots\ldots$$

Os números $a_1, a_2, \ldots$ são os *termos* da série e os $s_1, s_2, \ldots, s_n, \ldots$ são suas *somas parciais* (ou *reduzidas*).

Uma série $\sum_{i=1}^{\infty} a_i$ se diz *convergente* se a seqüência (s_n) de suas reduzidas converge para algum $s \in \mathbb{R}$. Neste caso o número s é chamado *soma* da série e escreve-se $\sum_{i=1}^{\infty} a_i = s$.

Exemplo 18: Mostremos que a série infinita

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = \sum_{n=1}^{\infty} \frac{1}{2^{n-1}}$$

converge em $\mathbb{R}$.

A seqüência de suas reduzidas é

$$s_1 = 1 = 2 - 1$$

$$s_2 = 1 + \frac{1}{2} = \frac{3}{2} = 2 - \frac{1}{2}$$

$$s_3 = 1 + \frac{1}{2} + \frac{1}{4} = \frac{7}{4} = 2 - \frac{1}{4}$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$s_n = 1 + \frac{1}{2} + \ldots + \frac{1}{2^{n-1}} = 2 - \frac{1}{2^{n-1}}$$

$$\ldots\ldots\ldots\ldots\ldots$$

Logo:

$$(s_n) = (2 - 1, 2 - \frac{1}{2}, 2 - \frac{1}{4}, \ldots, 2 - \frac{1}{2^{n-1}}, \ldots) = (2, 2, 2, \ldots) +$$

$$+ (-1)(1, \frac{1}{2}, \frac{1}{4}, \ldots, \frac{1}{2^{n-1}}, \ldots)$$

Como $(2, 2, 2, \ldots)$ converge para 2 e $\frac{1}{2^{n-1}}$ converge para 0, então (s_n) converge para

$$2 + (-1) \cdot 0 = 2$$

devido à proposição 5.

Exemplo 19: A chamada *série harmônica*

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots = \sum_{i=1}^{\infty} \frac{1}{i}$$

não é convergente. De fáto, observando que

$$\frac{1}{3} + \frac{1}{4} > \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

$$\frac{1}{5} + \ldots + \frac{1}{8} > 4 \cdot \frac{1}{8} = \frac{1}{2}$$

$$\frac{1}{9} + \ldots + \frac{1}{16} > 8 \cdot \frac{1}{16} = \frac{1}{2}$$

$$\vdots$$

então as somas parciais

$$s_n = 1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}} + \underbrace{\frac{1}{5} + \ldots + \frac{1}{8}} + \underbrace{\frac{1}{9} + \ldots + \frac{1}{16}} + \ldots \geqslant$$

$$\geqslant 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots$$

tornam-se arbitrariamente grandes quando n cresce indefinidamente. A notação seguinte é justificada por esse fato:

$$\sum_{i=1}^{\infty} \frac{1}{i} = +\infty$$

DEFINIÇÃO 7 Uma série infinita

$$\sum_{n=1}^{\infty} aq^{n-1} = a + aq + aq^2 + \ldots$$

onde a e q são números reais dados ($q \neq 0$), chama-se *série geométrica*.

PROPOSIÇÃO 7 Seja $q \in \mathbb{R}$ um número tal que $0 < q < 1$. Então a série geométrica $a + aq + aq^2 + \ldots$ converge, qualquer que seja $a \in \mathbb{Q}$, e sua soma é:

$$s = \frac{a}{1-q}$$

Demonstração: Para todo índice n, a enésima soma parcial da série considerada é

$$s_n = a + aq + \ldots + aq^{n-1}$$

Daí:

$$qs_n = aq + aq^2 + \ldots + aq^n$$

Subtraindo essas igualdades:

$$s_n - qs_n = a - aq^n = a(1 - q^n)$$

e portanto

$$s_n = \frac{a(1-q^n)}{1-q} = \frac{a}{1-q} + \frac{-a}{1-q} \cdot q^n$$

Assim:

$$(s_n) = \left(\frac{a}{1-q} + \frac{-a}{1-q} \cdot q, \frac{a}{1-q} + \frac{-a}{1-q} \cdot q^2, \ldots\right) =$$

$$= \left(\frac{a}{1-q}, \frac{a}{1-q}, \ldots\right) + \frac{-a}{1-q}(q, q^2, q^3, \ldots)$$

Como $\left(\frac{a}{1-q}, \frac{a}{1-q}, \ldots\right)$ converge para $\frac{a}{1-q}$ e (q^n) converge para 0 (exemplos 14 e 17), então (s_n) também converge e seu limite é

$$\lim s_n = \frac{a}{1-q} + \frac{-a}{1-q} \cdot 0 = \frac{a}{1-q}$$

devido à proposição 5. ■

DEFINIÇÃO 8 Toda série $\sum_{n=1}^{\infty} a_n$ de números reais determinada por uma seqüência tal que $a_n \geq 0$, $\forall n \geq 1$, recebe o nome de *série de termos positivos*.

A série harmônica, por exemplo, é uma série de termos positivos. O mesmo se pode dizer da série geométrica

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots$$

Notemos que se $\sum_{i=1}^{\infty} a_i$ é uma série de termos positivos, então a seqüência (s_n),

$$s_1 = a_1$$
$$s_2 = a_1 + a_2$$
$$s_3 = a_1 + a_2 + a_3$$
$$\ldots\ldots\ldots$$

de suas reduzidas é crescente. Logo, se (s_n) for limitada, então converge para algum $s \in \mathbb{R}$ que é, por definição, a soma da série.

PROPOSIÇÃO 8 Seja $\sum_{n=1}^{\infty} a_n$ uma série de termos positivos em $\mathbb{R}$. Se $\sum_{n=1}^{\infty} b_n$ é uma série convergente em $\mathbb{R}$ tal que $a_n \leq b_n$, para todo $n \geq 1$, então $\sum_{n=1}^{\infty} a_n$ também converge em $\mathbb{R}$.

Demonstração: Sejam $s_n = a_1 + \ldots + a_n$ e $t_n = b_1 + \ldots + b_n$, para qualquer $n \geq 1$. Como (t_n) por hipótese converge, então existe $k \in \mathbb{R}$ tal que

$$|t_n| < k, \forall n \geq 1$$

pois toda seqüência convergente é limitada. Mas $a_n \leq b_n$ $(n \geq 1)$ implica que

$$s_n = a_1 + \ldots + a_n \leq b_1 + \ldots + b_n = t_n$$

para todo $n \geq 1$. Então:

$$|s_n| = s_n \leq t_n = |t_n| < k \qquad (n \geq 1)$$

Assim (s_n) também é limitada e, como é crescente (pois é uma série de termos positivos), então existe $s \in \mathbb{R}$ tal que $s_n \to s$. Ou seja:

$$\sum_{n=1}^{\infty} a_n = s$$

■

Exemplo 20: Mostremos que toda série

$$\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} + \ldots$$

onde os a_i são inteiros, $0 \leq a_i \leq 9$, para todo $i \geq 1$, converge em $\mathbb{R}$ para um número positivo menor que ou igual a 1.

Observemos primeiro que:

$$\frac{a_n}{10^n} \leq \frac{9}{10^n} \quad (n \geq 1)$$

Mas $\sum_{n=1}^{\infty} \frac{9}{10^n} = \frac{9}{10} + \frac{9}{100} + \ldots$ é uma série geométrica de razão $q = \frac{1}{10}$ que, portanto, converge em $\mathbb{R}$ e cuja soma é

$$t = \frac{\frac{9}{10}}{1 - \frac{9}{10}} = 1$$

A proposição anterior nos garante então que a série dada converge em $\mathbb{R}$.

Como 1 é uma cota superior de $\{t_n | n \geq 1\}$, onde $t_n = \frac{9}{10} + \frac{9}{10^2} + \ldots + \frac{9}{10^n}$, então 1 também é cota superior de $\{s_n | n \geq 1\}$, $s_n = \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}$, e portanto a soma s da série dada é menor que ou igual a 1. Como cada termo da série é positivo, pode-se concluir que s também é positivo (justifique).

EXERCÍCIOS

479. Considere a série infinita $\sum_{n=1}^{\infty} \frac{1}{n(n+1)}$.

a) Se s_n é a enésima reduzida da série dada, mostre que $s_n = \frac{n}{n+1}$.

b) Mostre que a soma dessa série é igual a 1.

Sugestão para a): $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$.

480. Se uma série $\sum_{n=1}^{\infty} a_n$ converge, prove que $\lim a_n = 0$.

Resolução: Indiquemos por s_n ($n = 1, 2, 3, \ldots$) as reduzidas e por s a soma da série dada. Então $\lim s_n = s$ e portanto, dado $\varepsilon > 0$, existe um índice r tal que $|s - s_n| < \frac{\varepsilon}{2}$, $\forall n \geqslant r$. Assim, para todo $n \geqslant r$:

$|a_{n+1}| = |s_{n+1} - s_n| = |s - s_n + s_{n+1} - s| \leqslant |s - s_n| + |s_{n+1} - s| < \varepsilon$

Logo: $\lim a_n = \lim a_{n+1} = 0$

481. a) Dada a série $\sum_{n=1}^{\infty} a_n$, se $\lim a_n \neq 0$, prove que $\sum_{n=1}^{\infty} a_n$ é *divergente* ($\Longleftrightarrow$ não é convergente).

b) Mostre que são divergentes:

i) $\sum_{n=1}^{\infty} \frac{n^2+5}{n^2}$ ii) $\sum_{n=1}^{\infty} (-1)^{n+1} \cdot 5$ iii) $\sum_{n=1}^{\infty} \frac{n+1}{n+2}$

482. Seja $c \neq 0$ um número real.

a) Se $\sum_{n=1}^{\infty} a_n$ é convergente, prove que $\sum_{n=1}^{\infty} ca_n$ também é convergente; e que, se a soma de $\sum_{n=1}^{\infty} a_n$ é s, a de $\sum_{n=1}^{\infty} ca_n$ é cs.

b) Se $\sum_{n=1}^{\infty} a_n$ é divergente, mostre que $\sum_{n=1}^{\infty} ca_n$ também é divergente.

c) Mostre que $\sum_{n=1}^{\infty} \frac{1}{4n}$ é divergente.

483. Se $s = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \ldots$ ($a_1, a_2, \ldots, a_r, \ldots \in \mathbb{N}$; $0 \leqslant a_i \leqslant 9$), mostre que:

$$10^r s = a_1 a_2 \ldots a_r + \frac{a_{r+1}}{10} + \frac{a_{r+2}}{10^2} + \frac{a_{r+3}}{10^3} + \ldots$$

Resolução: $s = \lim_{n\to\infty}\left(\frac{a_1}{10} + \ldots + \frac{a_r}{10^r} + \frac{a_{r+1}}{10^{r+1}} + \ldots + \frac{a_n}{10^n}\right)$, por hipótese. Logo (usando a proposição 5):

$$10^r s = \lim_{n\to\infty}\left(10^{r-1}a_1 + 10^{r-2}a_2 + \ldots + a_r + \frac{a_{r+1}}{10} + \ldots + \frac{a_{r+n}}{10^n}\right) =$$

$$= \lim_{n\to\infty}\left(a_1 a_2 \ldots a_r + \frac{a_{r+1}}{10} + \frac{a_{r+2}}{10^2} + \ldots + \frac{a_{r+n}}{10^n}\right) =$$

$$= a_1 a_2 \ldots a_r + \lim_{n\to\infty}\left(\frac{a_{r+1}}{10} + \frac{a_{r+2}}{10^2} + \ldots + \frac{a_{r+n}}{10^n}\right) =$$

$$= a_1 a_2 \ldots a_r + \frac{a_{r+1}}{10} + \frac{a_{r+2}}{10^2} + \ldots + \frac{a_{r+n}}{10^n} + \ldots$$

484. Se $s = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \ldots$ ($a_1, a_2, \ldots \in \mathbb{N}$; $0 \leqslant a_i \leqslant 9$), mostre que:

$$\frac{1}{10^r}s = \frac{a_1}{10^{r+1}} + \frac{a_2}{10^{r+2}} + \frac{a_3}{10^{r+3}} + \ldots$$

485. Seja $\sum_{n=1}^{\infty} b_n$ uma série de termos positivos que sabemos ser divergente. Se (a_n) é uma seqüência em $\mathbb{R}$ tal que $a_n \geqslant b_n$, para todo índice n, prove que $\sum_{n=1}^{\infty} a_n$ também é divergente.

Resolução: Se $\sum_{n=1}^{\infty} a_n$ fosse convergente, pela proposição 8 a série $\sum_{n=1}^{\infty} b_n$ também teria que ser.

486. Mostre que $\sum_{n=1}^{\infty} \frac{1}{\sqrt{n}}$ é divergente.

Sugestão: Use o exercício anterior, comparando o termo genérico da série dada com o da série harmônica.

487. Mostre que a série $\sum_{n=1}^{\infty} \frac{4}{3^n + 1}$ é convergente.

Sugestão: Use a proposição 8 para comparar o termo genérico da série dada com o termo genérico de $\sum_{n=1}^{\infty} \frac{4}{3^n}$.

488. Deixa-se cair uma bola da altura de 4 m. Cada vez que a bola atinge o solo, após cair da altura de h m, volta uma distância de $\frac{3}{4}$ h m. Determine a distância total percorrida pela bola.

489. Se $\sum_{n=1}^{\infty} a_n$ e $\sum_{n=1}^{\infty} b_n$ são séries convergentes de soma s e t, respectivamente, mostre que $\sum_{n=1}^{\infty} (a_n \pm b_n)$ também converge e sua soma é $s \pm t$.

Resolução:

$$\sum_{n=1}^{\infty} (a_n \pm b_n) = \lim_{n \to \infty} \left(\sum_{j=1}^{n} (a_j \pm b_j) \right) =$$

$$= \lim_{n \to \infty} \left(\sum_{j=1}^{n} a_j \pm \sum_{j=1}^{n} b_j \right) = \lim_{n \to \infty} \sum_{j=1}^{n} a_j \pm \lim_{n \to \infty} \sum_{j=1}^{n} b_j =$$

$$= s \pm t.$$

490. Se $\sum_{n=1}^{\infty} a_n$ é convergente e $\sum_{n=1}^{\infty} b_n$ é divergente, mostre que $\sum_{n=1}^{\infty} (a_n + b_n)$ é divergente.

7. A representação decimal de um número real

Seja m um inteiro positivo qualquer e consideremos inteiros $a_1, a_2, \ldots$ tais que $0 \leqslant a_i \leqslant 9$ $(i = 1, 2, \ldots)$. Do que vimos ao final do parágrafo anterior podemos concluir que a série

$$m + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots$$

converge em IR. Ou seja, a soma dessa série é um número real α. Para indicar este número adota-se a notação

$$\alpha = m, a_1 a_2 a_3 \ldots$$

chamada *representação* (ou *forma*) *decimal* de α.

Se para todo índice r existe um índice $s \geqslant r$ tal que $a_s \neq 0$, então essa representação se diz *infinita*. Por exemplo, a representação decimal da soma da série

$$1 + \frac{0}{10} + \frac{2}{10^2} + \frac{0}{10^3} + \frac{2}{10^4} + \ldots$$

é infinita. Essa representação é:

$$1{,}020202\ldots$$

Caso contrário, existe um índice r tal que $a_r = a_{r+1} = \ldots = 0$. Quando isto ocorre, então

$$\alpha = m \quad \text{ou} \quad \alpha = m + \frac{a_1}{10} + \ldots + \frac{a_{r-1}}{10^{r-1}}$$

cuja representação decimal, introduzida no capítulo IV (6), ou seja,

$$\alpha = m \quad \text{ou} \quad \alpha = m, a_1 a_2 \ldots a_{r-1}$$

passa a se chamar *finita*, em contraposição ao caso anterior.

Das considerações anteriores resulta então que a soma de toda série

$$m + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} + \ldots$$

onde $m, a_1, a_2, \ldots \in \mathbb{Z}$, $m \geqslant 0$ e $0 \leqslant a_i \leqslant 9$ $(i = 1, 2, \ldots)$, admite uma representação decimal (finita ou infinita). Assim, toda expressão

$$m, a_1 a_2 a_3 \ldots$$

representa um número real positivo. Mostraremos a seguir que vale o recíproco desse fato.

TEOREMA 2 Se α é um número real positivo, então existem inteiros positivos m, $a_1, a_2, \ldots$, onde $0 \leqslant a_i \leqslant 9$, de maneira que

$$\alpha = m, a_1 a_2 a_3 \ldots$$

Demonstração: Seja $[\alpha] = m$. Então $m \leqslant \alpha < m + 1$. Se $\alpha = m$, então o próprio m é a representação procurada. Se, em vez disso, $m < \alpha < m + 1$, consideremos o maior dos números

$$m, m + \frac{1}{10}, m + \frac{2}{10}, \ldots, m + \frac{9}{10}$$

que não supera α. Se $m + \frac{a_1}{10}$ é esse número, então:

$$\alpha_1 = m + \frac{a_1}{10} \leqslant \alpha < m + \frac{a_1 + 1}{10} = \alpha_1'$$

Se $\alpha = \alpha_1$, então

$$\alpha = m, a_1$$

e a demonstração se encerra. Caso contrário, repete-se o raciocínio anterior, ou seja, toma-se o maior dos números

$$m + \frac{a_1}{10}, m + \frac{a_1}{10} + \frac{1}{100}, \ldots, m + \frac{a_1}{10} + \frac{9}{100}$$

que não supera α. Se $m + \frac{a_1}{10} + \frac{a_2}{100}$ é esse número, então:

$$\alpha_2 = m + \frac{a_1}{10} + \frac{a_2}{100} \leqslant \alpha < m + \frac{a_1}{10} + \frac{a_2 + 1}{100} = \alpha_2'$$

Se $\alpha = \alpha_2$, então:

$$\alpha = m, a_1 a_2$$

e nada mais há que fazer. Do contrário repete-se o mesmo procedimento.

Nessa linha de raciocínio pode ocorrer de, para algum r,

$$\alpha = m, a_1 a_2 \ldots a_r$$

o que conclui a demonstração. Se isto não acontece para nenhum r, observemos os seguintes subconjuntos de $\mathbb{R}$: $S = \{\alpha_1, \alpha_2, \ldots\}$ e $T = \{\alpha_1', \alpha_2', \ldots\}$. Obviamente, todo elemento de S é menor que todo elemento de T.

Por outro lado, dado $\varepsilon > 0$, seja $r > 0$ um número natural que verifica a desigualdade

$$\frac{1}{10^r} < \varepsilon$$

Então:

$$\alpha_r' - \alpha_r = \left(m + \frac{a_1}{10} + \ldots + \frac{a_{r-1}}{10^{r-1}} + \frac{a_r + 1}{10^r}\right) -$$

$$-\left(m + \frac{a_1}{10} + \ldots + \frac{a_{r-1}}{10^{r-1}} + \frac{a_r}{10^r}\right) = \frac{1}{10^r} < \varepsilon.$$

Como $\alpha_r \leqslant \alpha < \alpha_r'$, então $\alpha - \alpha_r < \alpha_r' - \alpha_r$ e portanto

$$\alpha - \alpha_r < \varepsilon$$

Considerando porém que para todo $n \geqslant r$ vale

$$\alpha_r \leqslant \alpha_n \leqslant \alpha$$

então:

$$\alpha - \alpha_n \leqslant \alpha - \alpha_r < \varepsilon$$

Levando em conta que $|\alpha - \alpha_n| = \alpha - \alpha_n$, então

$$|\alpha - \alpha_n| < \varepsilon, \text{ para todo } n \geqslant r.$$

Logo $\alpha_n \to \alpha$, ou seja

$$m + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots = \alpha$$

o que nos permite escrever:

$$\alpha = m, a_1 a_2 a_3 \ldots$$

■

Na representação decimal de um número $\alpha \geqslant 0$, $\alpha = m, a_1 a_2 a_3 \ldots$, m é sua *parte inteira*, a_1 é a *primeira casa decimal*, a_2 é a *segunda casa decimal*, e assim por diante.

Se $\alpha < 0$ e $|\alpha| = m, a_1 a_2 \ldots$ (finita ou infinita), entende-se por representação decimal de α a seguinte expressão:

$$\alpha = -m, a_1 a_2 \ldots = -(m, a_1 a_2 \ldots)$$

Assim, pelo que vimos neste item, todo número real α pode ser caracterizado por admitir uma representação decimal

$$m, a_1 a_2 a_3 \ldots \quad \text{ou} \quad -m, a_1 a_2 a_3 \ldots$$

finita ou infinita, onde $m, a_1, a_2, \ldots \in \mathbb{N}$ e $0 \leqslant a_i \leqslant 9$ $(i = 1, 2, \ldots)$.

Exemplo 21: Vamos obter a representação decimal do número $\alpha = \sqrt{3}$, até a terceira casa decimal, usando o procedimento desenvolvido na demonstração do teorema anterior, a título de ilustração.

Observemos primeiro que $m = [\alpha] = [\sqrt{3}] = 1$. Procuremos agora na seqüência

$$1,\ 1 + \frac{1}{10},\ 1 + \frac{2}{10},\ \ldots,\ 1 + \frac{9}{10}$$

ou seja, em

$$1;\ 1{,}1;\ 1{,}2;\ \ldots;\ 1{,}9$$

o maior número que não supera $\sqrt{3}$. Como $(1{,}7)^2 = 2{,}89$ e $(1{,}8)^2 = 3{,}24$, esse número é 1,7. Usando a notação do teorema: $a_1 = 7$.

Agora na seqüência

$$1 + \frac{7}{10},\ 1 + \frac{7}{10} + \frac{1}{100},\ \ldots,\ 1 + \frac{7}{10} + \frac{9}{100}$$

ou seja, em

$$1{,}7;\ 1{,}71;\ 1{,}72;\ \ldots;\ 1{,}79$$

procuremos o maior número que não supera $\sqrt{3}$. Como $(1{,}73)^2 = 2{,}9929$ e $(1{,}74)^2 = 3{,}0276$, esse número é 1,73. Assim $a_2 = 3$.

Agora vejamos em

$$1 + \frac{7}{10} + \frac{3}{100} + \frac{1}{1\,000},\ 1 + \frac{7}{10} + \frac{3}{100} + \frac{2}{1\,000},\ \ldots,$$
$$1 + \frac{7}{10} + \frac{3}{100} + \frac{9}{1\,000}$$

ou em

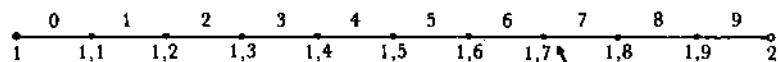
$$1{,}731;\ 1{,}732;\ 1{,}733;\ \ldots;\ 1{,}739$$

o maior número que não supera $\sqrt{3}$. Observando que $(1{,}732)^2 = 2{,}999824$ e $(1{,}733)^2 = 3{,}003289$, a resposta é 1,732. Assim $a_3 = 2$ e

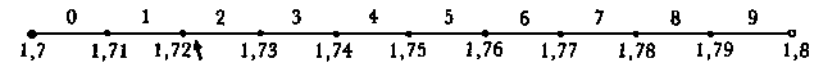
$$\sqrt{3} = 1{,}732\ \ldots$$

O processo que usamos pode ser visualizado da seguinte maneira:

Dividamos o intervalo $[1{,}2[$ em dez subintervalos de mesma amplitude que serão numerados de 0 a 9:

0 1 2 3 4 5 6 7 8 9
1 1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 1,9 2

Como $1{,}7 < \sqrt{3} < 1{,}8$, ou seja, como $\sqrt{3}$ pertence ao subintervalo ao qual associamos o numeral 7, então:

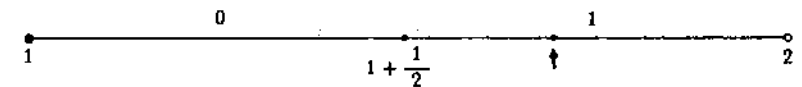
$$\sqrt{3} = 1{,}7\ \ldots$$

Agora devemos dividir $[1{,}7;\ 1{,}8[$ igualmente em 10 subintervalos de mesma amplitude, os quais também devem ser numerados de 0 a 9.

Como $1{,}72 < \sqrt{3} < 1{,}73$, então $\sqrt{3}$ pertence ao subintervalo assinalado com o numeral 2. Daí:

$$\sqrt{3} = 1{,}72\ \ldots$$

E assim por diante.

Exemplo 22: Assim como chegamos à representação decimal de um número $\alpha \in \mathbb{R}$, poderíamos, por exemplo, chegar à sua representação binária. Vejamos como isso poderia ser feito para $\sqrt{3} = \sqrt{(11)_2}$.

Evidentemente, a parte inteira de $\sqrt{(11)_2}$ é 1. Assim devemos dividir $[1{,}2[$ em dois subintervalos de mesma amplitude, aos quais atribuímos os dígitos 0 e 1 para numerá-los em ordem. Levando em conta que $\sqrt{3}$ pertence ao

segundo desses subintervalos, o que pode ser observado pela primeira figura do exemplo anterior, então:

$$\sqrt{(11)_2} = 1{,}1\ \ldots$$

Agora é o intervalo $[1 + \frac{1}{2},\ 2[$ que deve ser subdividido em dois de mesma amplitude, atribuindo-se ao primeiro o numeral 0 e ao segundo o numeral 1. Como $\sqrt{3}$ pertence ao primeiro desses subintervalos (ver as figuras do exemplo anterior), então:

$$\sqrt{(11)_2} = 1{,}10\ \ldots$$

8. A teoria da representação decimal em $\mathbb{Q}$

É bem conhecido o algoritmo que fornece a representação decimal de um número racional $\alpha = \frac{s}{t}$, onde t e s são inteiros estritamente positivos.

Por exemplo, se $\alpha = \frac{11}{6}$, então:

```
11   | 6
 50    1,833
  20
   20
    2
```

Ou seja:

$$\frac{11}{6} = 1,833\ldots$$

O lema a seguir justifica esse algoritmo a partir do teorema 2.

LEMA Seja $\alpha = \frac{s}{t}$ um número racional onde r e s são inteiros estritamente positivos. Se

$$\frac{s}{t} = m, a_1a_2a_3\ldots$$

é a representação decimal de α fornecida pelo teorema 2, então:

$a_1 = \left[\frac{10r_1}{t}\right]$, onde r_1 é o resto na divisão de s por t

$a_2 = \left[\frac{10r_2}{t}\right]$, onde r_2 é o resto na divisão de $10r_1$ por t

$a_3 = \left[\frac{10r_3}{t}\right]$, onde r_3 é o resto na divisão de $10r_2$ por t, ...

Demonstração: Se $\left[\frac{s}{t}\right] = m$, então $s = tm + r_1$ $(0 \leqslant r_1 < t)$. Como, de acordo com o teorema 2,

$$m + \frac{a_1}{10} \leqslant \frac{s}{t} = \frac{tm + r_1}{t} = m + \frac{r_1}{t} < m + \frac{a_1 + 1}{10}$$

então:

$$a_1 \leqslant \frac{10\,r_1}{t} < a_1 + 1$$

Daí, observando que a_1 e $a_1 + 1$ são inteiros consecutivos

$$a_1 = \left[\frac{10\,r_1}{t}\right]$$

Estabelecido assim que o resultado vale para a primeira casa decimal, a rigor deveríamos proceder por indução. Mas seremos informais. Provaremos apenas que também vale para a segunda casa decimal. O leitor perceberá, então, que o raciocínio pode ser repetido quantas vezes for necessário.

Levando em conta que $a_1 = \left[\frac{10\,r_1}{t}\right]$, então, aplicando o algoritmo da divisão para $10r_1$ e t

$$10\,r_1 = ta_1 + r_2\,(0 \leqslant r_2 < t)$$

Observando que

$$\frac{s}{t} - \left(m + \frac{a_1}{10}\right) = \frac{10s - 10tm - ta_1}{10t} = \frac{10r_1 - ta_1}{10t} = \frac{r_2}{10t}$$

pois $s = tm + r_1$ (daí $10s = 10tm + 10r_1$) e $10\,r_1 = ta_1 + r_2$, então:

$$\frac{s}{t} = m + \frac{a_1}{10} + \frac{r_2}{10t}$$

Logo, considerando o teorema 2:

$$m + \frac{a_1}{10} + \frac{a_2}{100} \leqslant m + \frac{a_1}{10} + \frac{r_2}{10t} < m + \frac{a_1}{10} + \frac{a_2 + 1}{100}$$

Dessas relações segue que

$$a_2 \leqslant \frac{10\,r_2}{t} < a_2 + 1$$

e portanto:

$$a_2 = \left[\frac{10\,r_2}{t}\right]$$

Analogamente

$$a_3 = \left[\frac{10\,r_3}{t}\right]$$

onde $10r_2 = ta_2 + r_3$ $(0 \leqslant r_2 < t)$, e assim por diante.

Observemos que como $a_1, a_2, a_3, \ldots$ são os quocientes da divisão euclidiana de $10r_1, 10r_2, 10r_3, \ldots$, respectivamente, por t, além de m ser o quociente da divisão de s por t, então o algoritmo pelo qual usualmente se chega à representação decimal de $\frac{s}{t}$ fica justificado. ■

Nota: Da demonstração anterior pode-se tirar, também, a seguinte conseqüência: $r_1, r_2, r_3, \ldots$ são os restos da divisão euclidiana de

$$s, 10s, 10^2s, \ldots$$

respectivamente, por t.

Quanto a r_1, não há o que provar, pois $s = tm + r_1$ $(0 \leqslant r_1 < t)$. Daí segue que:

$$10s = 10tm + 10r_1$$

Como porém $10r_1 = ta_1 + r_2$ $(0 \leqslant r_2 < t)$, então

$$10s = (10m + a_1)t + r_2 \quad (0 \leqslant r_2 < t)$$

e portanto na divisão euclidiana de 10s por t o resto é r_2.

Mas da última igualdade se obtém que:

$$10^2s = (10^2m + 10a_1)t + 10r_2$$

Levando em conta que $10r_2 = ta_2 + r_3$ $(0 \leqslant r_3 < t)$, então

$$10^2s = (10^2m + 10a_1 + a_2)t + r_3 \, (0 \leqslant r_3 < t)$$

e portanto nossa afirmação também é verdadeira no que toca a r_3. E assim por diante.

Exemplo 23: Voltemos ao número $\alpha = \dfrac{11}{6}$.

$$\begin{array}{rr|l} & 11 & 6 \\ \hline r_1 \rightarrow & 5 & 1 \leftarrow \left[\dfrac{11}{6}\right] = m \end{array}$$

Agora

$$\begin{array}{rr|l} & 11 & 6 \\ 10\,r_1 \rightarrow & 50 & 1{,}8 \\ r_2 \rightarrow & 2 & \uparrow \end{array} \qquad a_1 = \left[\frac{50}{6}\right] = \left[\frac{10\,r_1}{t}\right]$$

$$\begin{array}{rr|l} & 11 & 6 \\ & 50 & 1{,}83 \\ 10\,r_2 \rightarrow & 20 & \\ r_3 \rightarrow & 2 & \uparrow \end{array} \qquad a_2 = \left[\frac{20}{6}\right] = \left[\frac{10\,r_2}{t}\right]$$

Como $r_3 = r_2 = 2$, então todas as casas decimais seguintes serão iguais a 3.

8.1 Dízimas periódicas

Entendemos por *dízima periódica* toda representação decimal que se ajusta a um dos seguintes modelos (ambos infinitos):

$$m,\, a_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots$$

ou

$$m,\, b_1b_2 \ldots b_qa_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots$$

onde $m \geqslant 0$, $0 \leqslant a_i \leqslant 9$, $0 \leqslant b_j \leqslant 9$, com um dos a_i, pelo menos, não nulo.

O grupo de algarismos $a_1a_2 \ldots a_p$ chama-se *período* e o grupo $b_1b_2 \ldots b_q$ *anteperíodo* (ou *pré-período*) da dízima periódica. O número $p \geqslant 1$ é o *comprimento do período* e o número $q \geqslant 1$, o *comprimento do anteperíodo*.

Admitiremos sempre que o período tenha o menor comprimento possível. Por exemplo, em

$$0{,}25252525 \ldots$$

o período é 25 e não, digamos, 2 525 ou 252 525. E no caso de haver anteperíodo, exigiremos que $b_jb_{j+1} \ldots b_q \neq a_1a_2 \ldots a_p$, sempre que $1 \leqslant j \leqslant q$. Por exemplo em

$$0{,}1252525 \ldots$$

o anteperíodo é 1 e não, digamos, 125 ou 12 525.

Adotaremos, então, as seguintes notações:

$$m,\, a_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots = m,\, \overline{a_1a_2 \ldots a_p}$$

e

$$m,\, b_1b_2 \ldots b_qa_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots = m,\, b_1b_2 \ldots b_q\overline{a_1a_2 \ldots a_p}$$

Por exemplo:

$$2{,}3535 \ldots = 2{,}\overline{35}$$
$$8{,}63535 \ldots = 8{,}6\overline{35}$$
$$1{,}8333 \ldots = 1{,}8\overline{3}$$

TEOREMA 3 A representação decimal de um número racional estritamente positivo ou é finita ou é uma dízima periódica. Reciprocamente, as representações decimais finitas de parte inteira estritamente positivas e as dízimas periódicas representam sempre números racionais maiores que zero.

Demonstração:

$(\Rightarrow)$ Seja $\alpha = \dfrac{s}{t}$ $(s, t > 0)$ o número racional. Mantidas as notações do lema anterior e considerando a nota que o segue, os restos na divisão eucli-

diana de s, 10s, 10^2s, ... por t são $r_1, r_2, r_3, \ldots$ respectivamente. Admitamos que mdc(s, t) = 1 (isto sempre é possível).

Se, para um certo $k \geq 1$, $r_k = 0$, então $t \mid 10^{k-1}s$. No caso $k = 1$, se conclui que $t = 1$ e portanto α é inteiro; a representação decimal de α é o próprio s e portanto é finita. Se $k > 1$, como mdc(t, s) = 1, então $t \mid 10^{k-1}$ e portanto os fatores primos possíveis de t são 2 e 5, o que mostra que $\frac{s}{t}$ é um racional decimal; mas então

$$\frac{s}{t} = m + \frac{a_1}{10} + \ldots + \frac{a_p}{10^p}$$

e daí sua representação decimal é finita, ou seja:

$$\frac{s}{t} = m, a_1a_2 \ldots a_p$$

Suponhamos agora que $r_k \neq 0$ para todo $k \geq 1$. Ainda devido à nota ao lema anterior, podemos pôr

$$s \equiv r_1 \pmod t$$
$$10\,s \equiv r_2 \pmod t$$
$$10^2 s \equiv r_3 \pmod t$$
$$\vdots$$

Como nenhum dos r_i é nulo e $0 < r_i < t$ ($i = 1, 2, \ldots$), então há um primeiro índice $k + 1$, $k > 0$, de maneira que r_{k+1} é igual a um dos restos anteriores.

Admitamos inicialmente $r_{k+1} = r_1$. Então $10^k s \equiv r_1 \pmod t$ e portanto:

$$10^{k+1}s \equiv 10r_1 \equiv 10s \equiv r_2 \pmod t$$

Como

$$10^{k+1}s \equiv r_{k+2} \pmod t$$

e $0 < r_2, r_{k+2} < t$, então $r_{k+2} = r_2$. Analogamente se mostra que $r_{k+3} = r_3, \ldots, r_{2k} = r_k, r_{2k+1} = r_1, r_{2k+2} = r_2, \ldots, r_{3k} = r_k, \ldots$. Logo:

$$a_{k+1} = \left[\frac{10\,r_{k+1}}{t}\right] = \left[\frac{10\,r_1}{t}\right] = a_1$$

$$a_{k+2} = \left[\frac{10\,r_{k+2}}{t}\right] = \left[\frac{10\,r_2}{t}\right] = a_2$$

. . . .

$$a_{2k} = \left[\frac{10\,r_{2k}}{t}\right] = \left[\frac{10\,r_k}{t}\right] = a_k$$

$$a_{2k+1} = \left[\frac{10\,r_{2k+1}}{t}\right] = \left[\frac{10\,r_1}{t}\right] = a_1$$

. . . .

e portanto neste caso α não tem pré-período e seu período é $a_1a_2 \ldots a_k$ (comprimento k). Ou seja:

$$\alpha = \frac{s}{t} = m, \overline{a_1a_2 \ldots a_k}$$

No caso $r_{k+1} = r_{p+1}$ $(0 < p < k)$, se fizermos $k = p + q$, a mesma argumentação anterior nos levará à conclusão que

$$\alpha = m, a_1a_2 \ldots a_p\overline{a_{p+1}a_{p+2} \ldots a_{p+q}}$$

pois agora $a_{k+1} = a_{p+q+1} = a_{p+1}, \ldots, a_{k+q} = a_{p+q} = a_k$, etc. A dízima obtida tem então anteperíodo de comprimento p e período de comprimento q.

($\Leftarrow$) Dada uma representação decimal finita conforme o enunciado

$$m, a_1a_2 \ldots a_p$$

o número expresso por ela é:

$$m + \frac{a_1}{10} + \ldots + \frac{a_p}{10^p}$$

certamente um número racional.

No caso das dízimas, faremos a demonstração apenas para a hipótese de existir pré-período. Para a outra possibilidade, a argumentação é semelhante (veja-se exemplo 25 a seguir). Vamos supor, pois:

$$x = m, b_1b_2 \ldots b_q\overline{a_1a_2 \ldots a_p}$$
$$= m + 0, b_1b_2 \ldots b_q\overline{a_1a_2 \ldots a_p}$$

Multipliquemos

$$y = 0, b_1b_2 \ldots b_qa_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots$$

sucessivamente por 10^{q+p} e 10^q:

$$10^{q+p}y = b_1b_2 \ldots b_qa_1a_2 \ldots a_p, a_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots$$

$$10^q y = b_1b_2 \ldots b_q, a_1a_2 \ldots a_pa_1a_2 \ldots a_p \ldots$$

(Se o leitor tem alguma dúvida sobre a validade desse procedimento para multiplicação de dízimas por potências de 10, veja exercício 483). Então, subtraindo membro a membro essas igualdades (por que isso é possível?):

$$(10^{q+p} - 10^q)y = b_1b_2 \ldots b_qa_1a_2 \ldots a_p - b_1b_2 \ldots b_q$$

e daí:

$$y = \frac{b_1b_2 \ldots b_qa_1a_2 \ldots a_p - b_1b_2 \ldots b_q}{10^{q+p} - 10^q}$$

Como porém

$$10^{q+p} - 10^q = 10^q(10^p - 1) = 10^q \cdot 99\ldots9 = 99\ldots900\ldots0$$

onde o número de "noves" é p e o de "zeros" é q, então

$$y = \frac{b_1b_2\ldots b_qa_1a_2\ldots a_p - b_1b_2\ldots b_q}{99\ldots900\ldots0}$$

Observe-se que a fração em que y se transformou, demonstrando que $x = m + y$ representa um número racional maior que zero, tem tantos "noves" no denominador quantos são os algarismos do período e tantos "zeros" quantos são os algarismos do anteperíodo. ■

A fração em que se mostrou ser possível transformar y é chamada *geratriz* da dízima representada por y. Sua soma com m fornece uma geratriz de x.

Nota: Se a representação decimal de um número é finita, o mesmo se pode dizer da representação de seu oposto. Por exemplo:

$$\frac{5}{8} = 0{,}625 \Rightarrow -\frac{5}{8} = -0{,}625$$

E se a representação de um número é periódica, também a de seu oposto é periódica. **Por exemplo:**

$$\frac{59}{90} = 0{,}6555\ldots \Rightarrow -\frac{59}{90} = -0{,}6555\ldots$$

$$\frac{24}{99} = 0{,}2424\ldots \Rightarrow -\frac{24}{99} = -0{,}2424\ldots$$

Assim podemos concluir, em face do teorema anterior, que os números racionais se caracterizam por terem uma representação decimal finita ou infinita e periódica. Conseqüentemente os números irracionais se caracterizam por serem os números reais que, em sua representação decimal, têm expressões que nem são finitas e nem são periódicas.

Exemplo 24: Achemos a geratriz de $x = 1{,}24545\ldots$.

$$x = 1 + 0{,}24545\ldots =$$

$$= 1 + \frac{245-2}{990} = 1 + \frac{243}{990} = \frac{1\,233}{990}$$

Exemplo 25: Achemos a geratriz de $x = 0{,}\overline{357} = 0{,}357357\ldots$
Como $10^3x = 357{,}357357\ldots$, então $10^3x - x = 357$. Daí:

$$(10^3 - 1)x = 999x = 357$$

Donde:

$$x = \frac{357}{999}$$

PROPOSIÇÃO 9 Seja $\frac{s}{t} > 0$ uma fração ordinária irredutível cuja representação decimal é uma dízima periódica. Para que essa dízima não apresente pré-período é necessário e suficiente que $mdc(t, 10) = 1$. Neste caso o número de algarismos do período é a ordem de 10, módulo t.

Demonstração:

($\Rightarrow$) Se não há pré-período então, pelo que foi visto na demonstração do teorema 3 e mantidas as mesmas notações

$$10^ks \equiv r_1 \pmod t$$

onde $k + 1$ é o primeiro índice tal que $r_{k+1} = r_1$ e r_1 é o resto na divisão de s por t.

Como $s \equiv r_1 \pmod t$, então:

$$10^ks \equiv s \pmod t$$

Levando em conta que $mdc(s, t) = 1$ podemos cancelar s nessa congruência, resultando

$$10^k \equiv 1 \pmod t$$

onde $k \geqslant 1$. Daí segue que

$$10^k - tv = 1$$

para algum $v \in \mathbb{Z}$ e portanto $mdc(t, 10) = 1$.

($\Leftarrow$) Os elementos da seqüência

$$s,\ 10s,\ 10^2s,\ \ldots$$

não podem ser todos mutuamente incôngruos módulo t. Daí que para um par p, q de naturais, $p > q$, deve ocorrer

$$10^ps \equiv 10^qs \pmod t$$

Mas da hipótese $mdc(t, 10) = 1$ decorre que $mdc(t, 10^q) = 1$ e então podemos cancelar 10^q na última congruência:

$$10^{p-q}s \equiv s \pmod t$$

e daí

$$10^{p-q}s \equiv r_1 \pmod t$$

Mas

$$10^{p-q}s \equiv r_{p-q+1} \pmod t$$

Assim $r_{p-q+1} = r_1$ pois $0 < r_1, r_{p-q+1} < t$. Se $k+1$ é o primeiro índice para o qual $r_{k+1} = r_1$, então, de acordo com o teorema anterior

$$\frac{s}{t} = m, \overline{a_1 a_2 \ldots a_k}$$

o que prova esta recíproca, ou seja, $\frac{s}{t}$ não apresenta anteperíodo.

Mas se $r_{k+1} = r_1$ e $k+1$ é o menor índice nessas condições, então k é o menor expoente tal que $10^k \equiv 1 \pmod t$. De fato:

- se $r_{k+1} = r_1$, então $10^k s \equiv s \pmod t$ e cancelando s obtém-se que $10^k \equiv 1 \pmod t$;
- Se $10^n \equiv 1 \pmod t$, então $10^n s \equiv s \pmod t$ e daí $r_{n+1} = r_1$; logo $n+1 \geqslant k+1$ e $n \geqslant k$.

Então efetivamente k (período de $\frac{s}{t}$) é a ordem de 10, módulo t (ver cap. III, item 13). ■

Exemplo 26: Seja $t = 7$. Como $10 \equiv 3 \pmod 7$, $10^2 \equiv 2 \pmod 7$, $10^3 \equiv 6 \pmod 7$, $10^4 \equiv 4 \pmod 7$, $10^5 \equiv 5 \pmod 7$ e $10^6 \equiv 1 \pmod 7$, então a ordem de 10, módulo 7, é 6. Assim as frações $\frac{s}{7}$ em que $s > 0$ e $\text{mdc}(s, 7) = 1$ ($\iff 7 \nmid s$) são representadas por dízimas periódicas sem anteperíodo (pois $\text{mdc}(7, 10) = 1$) e com 6 algarismos no período. **Por exemplo:**

$$\frac{1}{7} = 0{,}142857142857\ldots = 0{,}\overline{142857}$$

PROPOSIÇÃO 10 Seja $\frac{s}{t}$ ($s > 0$ e $t > 0$) uma fração irredutível em que $t = n \cdot 2^\alpha \cdot 5^\beta$, $n > 1$, $\text{mdc}(n, 10) = 1$ e pelo menos um dos expoentes não é nulo. Então o pré-período da dízima periódica que representa $\frac{s}{t}$ tem comprimento $\gamma = \max\{\alpha, \beta\}$ e seu período tem comprimento igual à ordem de 10, módulo n.

Demonstração: Vamos manter ainda as notações do teorema 3 e do lema que o precede. Como há pré-período, se $k+1$ é o primeiro índice ($k \geqslant 1$) tal que r_{k+1} é igual a um dos restos anteriores e se p é o menor índice para o qual $r_{k+1} = r_{p+1}$, fazendo $k = p + q$, então $r_{p+q+1} = r_{p+1}$ (ver demonstração do teorema 3) e portanto

$$10^{p+q}s \equiv 10^p s \pmod t \qquad (*)$$

onde $t = n \cdot 2^\alpha \cdot 5^\beta$. Como $\text{mdc}(s, t) = 1$, então $\text{mdc}(s, 2^\alpha) = \text{mdc}(s, 5^\beta) = 1$.

Uma vez que da congruência anterior segue

$$n \cdot 2^\alpha \cdot 5^\beta \mid s \cdot 10^p \cdot (10^q - 1) \qquad (**)$$

então $2^\alpha \mid 10^p$ (pois 2^α é primo com s e com $10^q - 1 = 99\ldots9$) e $5^\beta \mid 10^p$ (por razões análogas). Daí $p \geqslant \alpha$ e $p \geqslant \beta$, o que implica $p \geqslant \gamma$.

Por outro lado, da relação (**) segue, observando que $\text{mdc}(n, 10) = 1$, que

$$n \mid s\,(10^q - 1)$$

Daí

$$2^\alpha \cdot 5^\beta \cdot n \mid s \cdot (10^q - 1) \cdot 10^\gamma$$

pois $\gamma \geqslant \alpha$ e $\gamma \geqslant \beta$. Esta última relação pode, contudo, ser expressa por

$$10^{\gamma+q}s \equiv 10^\gamma s \pmod t$$

da qual resulta $r_{\gamma+q+1} = r_{\gamma+1}$; se $\gamma < p$, ficaria contrariada a hipótese de que r_{k+1} é o primeiro resto igual a um dos anteriores; logo, $\gamma \geqslant p$.

Donde $\gamma = p$, o que garante a primeira afirmação da proposição, ou seja, que o anteperíodo de $\frac{s}{t}$ tem comprimento γ.

Da congruência (*), observando primeiro que $\text{mdc}(s, t) = \text{mdc}(s, n \cdot 2^\alpha \cdot 5^\beta) = 1$, resulta que

$$10^p \cdot 10^q \equiv 10^p \pmod t$$

e daí que:

$$n \mid 10^p\,(10^q - 1)$$

Como $\text{mdc}(n, 10) = 1$ e portanto $\text{mdc}(n, 10^p) = 1$, então

$$n \mid (10^q - 1)$$

ou

$$10^q \equiv 1 \pmod n$$

Agora, se

$$10^u \equiv 1 \pmod n$$

como $2^\alpha \cdot 5^\beta \mid 10^p$ (pois $p = \gamma$), então

$$10^{p+u} \equiv 10^p \pmod t$$

o que implica

$$10^{p+u}s \equiv 10^p s \pmod t$$

e portanto $r_{p+u+1} = r_{p+1}$. Considerando a escolha de $k = p + q$, então $u \geqslant q$.

Logo, q é de fato a ordem de 10 módulo n. Como q é o comprimento do período, a demonstração está concluída. ■

Exemplo 27: Consideremos as frações irredutíveis e estritamente positivas, de denominador $12 = 2^2 \cdot 3$.

Como o 5 não é fator primo de 12, então $\beta = 0$ e portanto $\gamma = \max\{0, \alpha = 2\} = 2$. Logo, essas frações têm como representação decimal dízimas com dois algarismos no pré-período. Por outro lado, observando que $10 \equiv 1 \pmod 3$, a ordem de 10, módulo 3, é 1 e cada uma dessas dízimas tem apenas um algarismo no período. Por exemplo:

$$\frac{1}{12} = 0{,}08333\ldots$$

EXERCÍCIOS

491. Determine a representação decimal dos números $\sqrt{5}$, $\sqrt{7}$ e $\sqrt[3]{2}$, até a terceira casa após a vírgula, usando o procedimento do teorema 2.

492. Determine geometricamente a representação binária dos números $\sqrt{5}$, $\sqrt{7}$ e $\sqrt[3]{2}$, até a terceira casa após a vírgula.

493. Ache as geratrizes das seguintes dízimas periódicas:

a) $0{,}0444\ldots$ d) $1{,}0\overline{2}$
b) $2{,}131313\ldots$ e) $24{,}24424242\ldots$
c) $1{,}4\overline{76}$ f) $0{,}01\overline{672}$

494. Determine o número de algarismos do período da representação decimal das frações ordinárias irredutíveis cujos denominadores são:

a) 11 b) 13 c) 17 d) 21

495. Determine o comprimento do anteperíodo e o do período da representação decimal de $\frac{1}{n}$ nos seguintes casos:

a) $n = 3 \cdot 5^2$ d) $n = 42$
b) $n = 2 \cdot 3^2 \cdot 5$ e) $n = 63$
c) $n = 105$ f) $n = 190$

496. Seja $\frac{m}{n}$, $0 < \frac{m}{n} < 1$, uma fração irredutível.

a) Determine todos os possíveis valores de $n > 1$ de maneira que a representação decimal desse número seja infinita, com um algarismo no pré-período e dois no período.
b) Tomando para n a menor das soluções encontradas em a), qual o valor de m para o qual o pré-período seja 3?

Resolução:

a) Como há anteperíodo, então $\text{mdc}(n, 10) \neq 1$ e portanto $n = k \cdot 2^\alpha \cdot 5^\beta$, onde $k \neq 2$ e $k \neq 5$, $k > 1$ (se $k = 1$, $\frac{m}{n}$ seria um número racional decimal) e um dos expoentes é maior que zero (lembrar que o comprimento do pré-período é igual a $\max\{\alpha, \beta\}$). Observando porém que

$$1 = \text{número de algarismos do pré-período} = \max\{\alpha, \beta\}$$

então $n = 2k$, $n = 5k$ ou $n = 10k$. Além disso

$$2 = \text{número de algarismos do período} = \text{ordem de 10, módulo k.}$$

Observando que $10^2 \equiv 1 \pmod k$ implica que $k \mid 99$, então k deve ser procurado entre 3, 9, 11, 33 ou 99. Como $10^1 \equiv 1 \pmod 3$ e $10^1 \equiv 1 \pmod 9$, 10 tem ordem 1 módulo 3 e módulo 9; assim 3 e 9 devem ser descartados. Restam $k = 11$, 33 ou 99.
Donde: $n = 22$, 66, 198, 55, 165, 495, 110, 330 ou 990.

b) Supondo $\frac{m}{n} = 0{,}a\overline{bc}$, devemos impor que

$$\frac{m}{22} = 0{,}3\,\overline{bc} = \frac{3bc - 3}{990} = \frac{c + 10b + 100 \cdot 3 - 3}{990} = \frac{297 + bc}{990}$$

o que leva a

$$m = \frac{297 + bc}{45}$$

Como m deve ser inteiro:

$$bc \equiv -297 \equiv 18 \pmod{45}$$

Considerando que bc é formado de dois algarismos (b e c), então $bc = 18$ ou $bc = 63$. Daí $m = 7$ ou $m = 8$. Como $\frac{m}{n}$ deve ser irredutível, a fração procurada é

$$\frac{7}{22} = 0{,}31818\ldots$$

497. Considere uma fração irredutível $\frac{m}{n}$ tal que $0 < \frac{m}{n} < 1$ e n é formado por dois algarismos.

a) Determine todos os valores possíveis de $n > 1$ a fim de que a representação decimal desse número seja infinita com um algarismo no anteperíodo e três no período.
b) Tomando para n a menor das soluções encontradas em a), determine m a fim de que o pré-período seja 8.

498. Considere a fração $\frac{1}{n}$, onde $n = 3 \cdot 10^{\alpha}$ $(\alpha \geqslant 1)$.

a) Qual o comprimento do pré-período de $\frac{1}{n}$?

b) Dado $\beta \in \mathbb{N}$, $\beta \geqslant 1$, determine a relação entre os pré-períodos de $\frac{1}{n}$ e $\frac{1}{n^{\beta}}$.

c) Determine β de maneira que o pré-período e o período de $\frac{1}{n^{\beta}}$ tenham três algarismos.

499. Determine os possíveis valores de $n > 1$ a fim de que $\frac{1}{n}$ gere uma dízima periódica simples (sem anteperíodo) e: a) seu período tenha comprimento 2; b) seu período tenha comprimento 4.

500. Considere uma dízima periódica gerada por uma fração irredutível $\frac{m}{n}$ tal que mdc $(n, 9) = 1$. Mostre que o período da dízima é divisível por 9.

Resolução: Podemos supor $m < n$. Assim, seja $0, b_1 b_2 \ldots b_s \overline{c_1 c_2 \ldots c_t}$ a representação decimal de $\frac{m}{n}$. Logo (ver demonstração do teorema 3):

$$\frac{m}{n} = \frac{b_1 b_2 \ldots b_s c_1 c_2 \ldots c_t - b_1 b_2 \ldots b_s}{99 \ldots 900 \ldots 0}$$

onde o número de "noves" é t e o de "zeros" é s. Observando que

$$b_1 b_2 \ldots b_s c_1 c_2 \ldots c_t = c_1 c_2 \ldots c_t + 10^t \cdot (b_1 b_2 \ldots b_s)$$

e fazendo $c_1 c_2 \ldots c_t = P$ e $b_1 b_2 \ldots b_s = A$, então $(99 \ldots 900 \ldots 0) \cdot m =$
$= n[c_1 c_2 \ldots c_t + 10^t \cdot (b_1 b_2 \ldots b_s) - b_1 b_2 \ldots b_s] =$
$= n[P + A(10^t - 1)]$

Como $9 | 99 \ldots 900 \ldots 0$, então 9 divide $n[P + A(10^t - 1)]$. Mas sendo primo com n, 9 é divisor de $P + A(10^t - 1)$. Levando em conta que $10^t - 1 = 99 \ldots 9$ é múltiplo de 9, então $9 | P$.

501. Considere uma dízima periódica gerada pela fração irredutível $\frac{m}{n}$. Se o número de algarismos do período é par e mdc$(n, 11) = 1$, mostre que o período é múltiplo de 11.

502. Mostre que:

a) $0,999 \ldots = 1$
b) $1,24999 \ldots = 1,25$
c) $0,334999 \ldots = 0,335$
d) $4,2 = 4,1999 \ldots$
e) Se $m > 0$ e $a = m, 999 \ldots$, então $a = m + 1$

503. Seja $p > 1$ um número primo diferente de 2 e de 5. Mostre que se o período da dízima gerada por $\frac{1}{p}$ tem um número par de algarismos, digamos $\frac{1}{p} = 0, \overline{a_1 a_2 \ldots a_{2t}}$, então $a_1 + a_{t+1} = a_2 + a_{t+2} = \ldots = a_t + a_{2t} = 9$. **Por exemplo:**
$\frac{1}{7} = 0,\overline{142857}$, onde $1 + 8 = 4 + 5 = 2 + 7 = 9$

Sugestão: Por hipótese, 2t é o menor expoente estritamente positivo tal que $10^{2t} \equiv 1 \pmod{p}$. Daí $(10^t - 1)(10^t + 1) \equiv 0 \pmod{p}$ e portanto $10^t + 1 \equiv 0 \pmod{p}$. Isso obriga $\frac{10^t + 1}{p} = \frac{1}{p} + 10^t \cdot \frac{1}{p}$ a ser um número inteiro.

504. Seja $\frac{m}{n}$ uma fração irredutível que gera uma dízima periódica com um pré-período de s algarismos.

a) Mostre que a representação decimal de $\frac{m^2}{n^2}$ também apresenta pré-período.

b) Prove que o pré-período de $\frac{m^2}{n^2}$ é formado de 2s algarismos.

Resolução de b): Da hipótese segue que $n = k \cdot 2^{\alpha} \cdot 5^{\beta}$, onde $k > 1$, mdc$(k, 10) = 1$ e pelo menos um dos expoentes não é nulo. Além disso: $s = \max\{\alpha, \beta\}$. Como

$$\frac{m^2}{n^2} = \frac{m^2}{k^2 \cdot 2^{2\alpha} \cdot 5^{2\beta}}$$

e as condições da proposição 10 se verificam para o denominador da última fração, então o pré-período de $\frac{m^2}{n^2}$ tem

$$\max\{2\alpha, 2\beta\} = 2 \max\{\alpha, \beta\} = 2s$$

algarismos.

505. Seja $n > 1$ um inteiro.

a) Mostre que se a fração $\dfrac{n^2+1}{n(n^2-1)}$ não é irredutível, então $\text{mdc}(n^2+1,\ n(n^2-1)) = 2$.

b) Mostre que, em qualquer caso, sua representação decimal é infinita e apresenta pré-período.

Sugestão para b): Mostre que, mesmo quando se dividem numerador e denominador por 2 (na hipótese em que isto é possível), o denominador obtido é múltiplo de 6.

506. Mostre que para todo inteiro n, $n \neq -2$, $n \neq -1$ e $n \neq 0$, a representação decimal de

$$\frac{1}{n} + \frac{1}{n+1} + \frac{1}{n+2}$$

apresenta pré-período.

507. Seja α um número real. Se $n > 1$ é um inteiro, mostre que existe um número racional $\dfrac{p}{q}$, $1 \leqslant q \leqslant n$, para o qual:

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{qn}$$

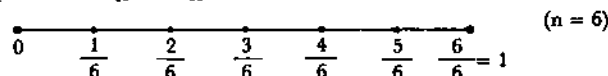
Resolução: Usaremos o *princípio da casa dos pombos* ou *princípio das gavetas de Dirichlet* cujo enunciado é o seguinte: "Se $n + 1$ objetos são colocados em no máximo n gavetas, então uma delas pelo menos ficará com mais do que um desses objetos".

Consideremos os $n + 1$ números $0 = 0 \cdot \alpha$, $\alpha - [\alpha]$, $2\alpha - [2\alpha]$, ..., $n\alpha - [n\alpha]$, todos do intervalo $[0, 1]$.

Dividamos este intervalo em n subintervalos por meio dos pontos

$$0 = \frac{0}{n},\ \frac{1}{n},\ \ldots,\ \frac{n-1}{n},\ \frac{n}{n} = 1.$$

(n = 6)

$0 \quad \frac{1}{6} \quad \frac{2}{6} \quad \frac{3}{6} \quad \frac{4}{6} \quad \frac{5}{6} \quad \frac{6}{6} = 1$

Estes n subintervalos são as gavetas onde estão os $n + 1$ números $k\alpha - [k\alpha]$ $(0 \leqslant k \leqslant n)$. Logo dois desses números, digamos $r\alpha - [r\alpha]$ e $s\alpha - [s\alpha]$, $0 \leqslant r < s \leqslant n$, estão na mesma gaveta, o que significa que a distância entre eles é $\leqslant \dfrac{1}{n}$. Fazendo $s - r = q$ e $[s\alpha] - [r\alpha] = p$, então:

$$|q\alpha - p| = |(s-r)\alpha - ([s\alpha] - [r\alpha])| =$$

$$= |(s\alpha - [s\alpha]) - (r\alpha - [r\alpha])| \leqslant \frac{1}{n}$$

Daí segue que:

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{nq}$$

Para concluir, observemos que $0 \leqslant r < s \leqslant n \Rightarrow 1 \leqslant q = s - r \leqslant s \leqslant n$.

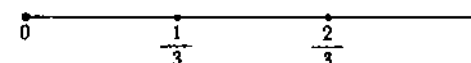
508. O exercício anterior fornece um método de aproximação de números irracionais por números racionais. Use esse método nos seguintes casos:

a) $\alpha = \sqrt{2}$ e $n = 3$

b) $\alpha = \sqrt{3}$ e $n = 4$

c) $\alpha = \pi$ e $n = 6$

d) $\alpha = e = 2{,}718281\ldots$ e $n = 5$.

Resolução de a): Como $\sqrt{2} = 1{,}414213\ldots$, devemos considerar os 4 números: $0 = 0 \cdot \sqrt{2}$; $\sqrt{2} - [\sqrt{2}] = 0{,}41421\ldots$; $2\sqrt{2} - [2\sqrt{2}] = 0{,}82842\ldots$; $3\sqrt{2} - [3\sqrt{2}] = 0{,}24264\ldots$ que estão no intervalo

o primeiro e o último no subintervalo $[0, \frac{1}{3}]$. Logo, mantendo a notação do exercício anterior: $r = 0$ e $s = 3$ e daí $q = s - r = 3$ e $p = [3\alpha] - [0\alpha] = [3\sqrt{2}] - [0] = 4$. Assim, o número racional fornecido pelo processo é $\dfrac{4}{3}$ e

$$\left|\sqrt{2} - \frac{4}{3}\right| \leqslant \frac{1}{9}$$

RESPOSTAS A EXERCÍCIOS NUMÉRICOS E TESTES

CAPÍTULO I

1. a)

c)

b)

d)

2. a) 538

b) 1 263

c) 1 035

3. a)

b)

c)

d)

4. a) 63

b) 132

c) 72 310

d) 252 142

5. a) 47°21'7''

b) 10°58'43''

c) 136°56'9''

d) 7°3'21''

6. a) $\tau ϙ \eta$

b) $`\alpha\sigma\varkappa\gamma$

c) $`\theta\varrho\varkappa\eta$

d) $\overset{\beta}{M}\tau ϙ \beta$

7. a) 381

b) 298

c) 12 219

d) 30 333

9. a) MCDXCII

b) MCMXCVIII

c) $\overline{LXXIV}DCCCXII$

d) $\overline{\overline{III}}\overline{CXLII}CCXXXVI$

10. a) 124

b) 1 748

c) 19 000

d) 90 000 025

16. a) 56 = 1 + 10 + 45

b) 69 = 3 + 21 + 45

c) 287 = 6 + 28 + 253

CAPÍTULO II

21. a) 32

b) 47

c) $\frac{3(r+2)(r+3)}{2}$

d) 14

22. a) 625

b) 36

c) 1 411 200

d) 19 683

23. a) $\sum_{i=1}^{3} (a_i + i + 1)$

b) $\sum_{r=2}^{n} r^{r+1}$

c) $\prod_{i=1}^{19} (6 + i)$

d) $\sum_{i=1}^{n} a_i b_{i+1}$

e) $\sum_{i=1}^{n} i^2$

f) $\sum_{i=1}^{p} 2^i$

24. c

33. d

35. 111 e 2 250

36. d

45. não

46. $(10110110)_2$; $(266)_8$; $(132)_{12}$

47. a) $(1332)_5$ b) $(52124)_6$ c) $(210012)_4$

48. 97; 147; 1 859

49.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	11	13	15
3	0	3	6	12	15	21	24
4	0	4	11	15	22	26	33
5	0	5	13	21	26	34	42
6	0	6	15	24	33	42	51

50. a) $b = 91$ b) $b = 8$

53. $1 - b + b^2 = 1 + (b-1)b = ((b-1)1)_b$

55. $b = 2(d-1)$; $d > 3$

57. d **58.** 234 **59.** b) 13 **60.** 8

61. $(b-1)b^{n-1}$ e b^{n-1}

62. a) 4 e 22 680 b) 4 e 10 560

64. 500 e 180

66. (20 e 240) ou (60 e 80)

72. c **80.** 420 anos **81.** 264, 528 e 792

82. 1 150 **83.** c **85.** 48 e 72

87. a) 20 b) $r \leqslant 5$, $s = 0$ e $t \leqslant 2$

88. a) $2 \cdot 19^2 \cdot 71$
b) $5 \cdot 31 \cdot 131$
c) $3^2 \cdot 11^2 \cdot 113$

89. i) $3^2 \cdot 19$
ii) $2 \cdot 19$
iii) 19
iv) $2^4 \cdot 3^2 \cdot 19^2 \cdot 71^2$
v) $2 \cdot 3^5 \cdot 19 \cdot 61 \cdot 71^2$

90. b **91.** Sim; não; sim.

92. 11 e $2^2 \cdot 11^2 \cdot 29^3$; $2^2 \cdot 11$ e $11^2 \cdot 29^3$; $11 \cdot 29^3$ e $2^2 \cdot 11^2$

94. a

105. a) 144

108. $\alpha = 2$ e $\beta = 6$ ou $\alpha = 6$ e $\beta = 2$

111. $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6$
$\sigma(6) = 12, \sigma(7) = 8, \sigma(8) = 15, \sigma(9) = 13, \sigma(10) = 18$

116. a) Abundante: 12. Deficientes: 1, 2, 3, 4, 5, 7, 8, 9, 10 e 11. Perfeito: 6.
b) Todos são deficientes.

123. (90, 56, 106); (220, 21, 221); (140, 51, 149); (132, 85, 157)

124. a) (12, 5, 13) e (12, 35, 37)
b) (15, 8, 17)

134. $mdc(f_9, f_{12}) = f_3 = 2$; $mdc(f_{15}, f_{20}) = f_5 = 5$
$mdc(f_{24}, f_{36}) = f_{12} = 144$

136. De f_{16}: f_1, f_2, f_4, f_8 e f_{16}
De f_{30}: $f_1, f_2, f_3, f_5, f_6, f_{10}, f_{15}, f_{30}$

137. Falso.

143. $f_1, f_2, f_4, f_8, f_{10}$

CAPÍTULO III

172. a) $q = 5, r = 20$
b) $q = -7, r = 2$
c) $q = -8, r = 44$

173. $(b = 23, r = 4)$ ou $(b = 22, r = 18)$

175. a) $a = 630, b = 105$
b) $a = 201, b = 33$

176. 9 994 e 1 007

193. a) 4
b) 204
c) 2
d) 740
e) 378
f) 9 240

194. a) 5
b) 11 115
c) 1
d) $3^2 \cdot 5^2 \cdot 13 \cdot 19 \cdot 41 = 2 \cdot 278 \cdot 575$

195. $\{6k + 1 | k \in \mathbb{Z}\} \cup \{6k + 5 | k \in \mathbb{Z}\}$

196. 1 ou 7

197. a) $b = 63 - 9s$, $7 \nmid s$
b) $b = 4r - 20$, $5 \nmid r$
c) $b = 45$ ou $b = -60$
d) $b = \pm 8, \pm 72$

210. $x_0 = 8$, $y_0 = 13$

211. $x_0 = 12$, $y_0 = -25$

217. $b = 9$

218. $\pm 198, \pm 297, \pm 396, \pm 495, \pm 594, \pm 693, \pm 792, \pm 891, \pm 990$

223. a) $-2^2 \cdot 5 \cdot 11 \cdot 131$
b) $-3^2 \cdot 31 \cdot 47 \cdot 101$
c) $-109 \cdot 113$
d) $-2^2 \cdot 499$

224. a) sim b) não c) não d) sim

227. 3 e -3

235. $a = 62\,500$ $b = 1\,250$

237. $f(16) = 289 = 17^2$; $g(18) = 703 = 19 \cdot 37$
$h(22) = 1\,541 = 23 \cdot 67$

245. $50! = 2^{47} \cdot 3^{22} \cdot 5^{12} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$

250. a) $x = -20 + 4t$, $y = 20 - 3t$
b) $x = -2 - 2t$, $y = -6 - 5t$
c) $x = 18 + 23t$, $y = -3 - 4t$
d) $x = 4 - 10t$, $y = 4 - 9t$
e) $x = -10 + 3t$, $y = -5 + 2t$
f) $x = -22 - 9t$, $y = -11 - 4t$

251. 44 e 56

253. 197 crianças e 1 adulto.

254. 6 e 10, respectivamente.

255. US\$180; 13 notas de US\$10 e 1 (uma) de US\$50.

256. a) $x = -15\,368 + 19t$; $y = 5\,763 - 7t$
b) (3, 100)

257. 9 cavalos e 71 bois.

258. Respectivamente: $9 - 79t$ e $4 - 37t$ ($t \leqslant 0$).

259. a) 8 b) infinitas

260. a) $(-40, 20, 4)$
b) impossível
c) $(38, -24, 0)$
d) $(-10, 15, 0)$

262. a) 5, 13, 21, 29, ..., 109
b) 104, 111, 118, ..., 195

263. $m > 1$, $m | 252$

264. a) 1 b) 1 d) 0 e) 2

266. 0 (zero) **268.** 3 **270.** 9 **272.** 43

288. a) não b) sim c) não d) não e) sim

290. $x = 3$, $y = 2$

292. a) {16}
b) {4}
c) {45, 94}
d) {6, 13, 20}
e) ∅
f) {6, 30}
g) {5}
h) {17}

293. a) $x \equiv 52 \pmod{105}$
b) $x \equiv 208 \pmod{315}$
c) $x \equiv 67 \pmod{70}$
d) $x \equiv 82 \pmod{105}$
e) $x \equiv 268 \pmod{385}$

294. $x = 4\,128 + 6\,061\,k$ ($k \in \mathbb{Z}$)

295. $x \equiv 1103 \pmod{2210}$

296. 5. ***Obs.***: É possível que a resposta considerada por Yih-Hing tenha sido 17, partindo do pressuposto de que o dividendo devesse ser maior que o divisor, em qualquer caso.

298. 539

299. 3 930

300. a) $x \equiv 7 \cdot 1 \cdot 143 + 5 \cdot 4 \cdot 130 + 11 \cdot 6 \cdot 110 \pmod{1430}$
b) $x \equiv 26 \pmod{630}$

301. $x \equiv 52 \pmod{360}$

302. 79, 80 e 81 (por exemplo)

303. $\varphi(200) = 80$; $\varphi(860) = 336$; $\varphi(1\,001) = 720$

315. b) $5x \equiv 21 \pmod{14} \Rightarrow x_0 = 5^5 \cdot 21 \equiv 7 \pmod{14}$
$21x \equiv 30 \pmod{25} \Rightarrow x_0 = 2^{19} \cdot 30 \equiv 5 \pmod{25}$

318. a) 4 c) 25

321. i) $\mu(4) = 0$, $\mu(12) = 0$, $\mu(86) = 1$, $\mu(105) = -1$ e $\mu(120) = 0$

322. De 7: 1, 2 e 4
De 13: 1, 3, 4, 9, 10 e 12
De 17: 1, 2, 4, 8, 9, 13, 15 e 16

323. Respectivamente: v, f, v, f.

333. a) Módulo 17: respectivamente 4, 16 e 16.
b) Módulo 25: respectivamente 10, 4 e 5.
c) Módulo 15: respectivamente 2, 4 e 2.

361. a) $x \equiv 8 \cdot 7 \equiv 10 \pmod{23}$
b) $x \equiv 4 \pmod{15}$
c) $x \equiv 4 \cdot 3 \equiv 12 \pmod{19}$
d) $x \equiv 15 \pmod{17}$

363. a) Y J T W N F E I T X E S Z R J W T X
b) CAMPOS NUMÉRICOS

CAPÍTULO IV

366. $\frac{28}{20}$

367. $\frac{69}{253}$

368. $\frac{-52 + 5t}{5}$ e $\frac{78 - 7t}{7}$ $(t \in \mathbb{Z})$

370. não

373. a) $r = -2, 0, 1$ ou 3 b) $r = 4$

381. $r = -216 - 9k$ e $s = -108 - 4k$ $(k \neq -27$ e $k \neq -24)$

386. $\frac{13}{20} = \frac{1}{2} + \frac{1}{7} + \frac{1}{140}$; $\frac{4}{15} = \frac{1}{4} + \frac{1}{60}$

$\frac{9}{24} = \frac{1}{3} + \frac{1}{8}$; $\frac{7}{52} = \frac{1}{8} + \frac{1}{104}$

387. b) 1

390. b) $\frac{36}{54}$, $\frac{15}{75}$, $\frac{20}{70}$

392. $r = 3$ e $r = 1$, respectivamente.

395. a) 2 b) -2 c) $m - 1$
d) 1 se $m > 0$ e 0 se $m < 0$.

402. a) 0,00390625; d) $-0{,}0125$

403. b) $-\frac{60\,001}{10\,000}$ d) $-\frac{2\,801}{20\,000}$

404. b) 3, 2

405. $d < a < b < c$

408. Respectivamente: $(0{,}1111)_2$ e $(0{,}5343)_6$.

409. Respectivamente: 3,515625 e $(0{,}11100001)_2$.

410. b

411. Respectivamente: não existem e $x = y = 1$.

412. a) 7,2525 horas c) 12 h 9 min

414. a) 38% b) ii; c) Aproximadamente 38,29 km.

CAPÍTULO V

418. a) $-10 \in \varrho(3) \cap \varrho(-1) \cap \varrho(20, 1) \cap \varrho(\frac{1}{4})$

$0 \in \varrho(3) \cap \varrho(20, 1) \cap \varrho(\frac{1}{4})$

$\frac{2}{3} \in \varrho(3) \cap \varrho(20, 1)$

$\frac{5}{2} \in \varrho(3) \cap \varrho(20, 1)$

$20 \in \varrho(20, 1)$

b) $\frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{64}, \frac{1}{128}$

428. $1 + \sqrt{2}$ e $\sqrt{2}$, por exemplo.

429. $3\sqrt{2}$ e $2\sqrt{2}$

468. Todos têm a mesma cardinalidade de $\mathbb{R}$.

476. i) a) crescente e) decrescente
b) decrescente f) crescente

ii) Todas.

iii) a) : $\frac{3}{4}$ e) : 0

b) : $\frac{1}{25}$ f) : 1

488. 16 m

492. $\sqrt{5} = ((10)_2, 001 \ldots)_2$; $\sqrt{7} = ((10)_2, 101 \ldots)_2$; $\sqrt[3]{2} = (1{,}010 \ldots)_2$

493. a) $\frac{4}{90} = \frac{2}{45}$ d) $\frac{92}{90}$

b) $\frac{211}{99}$ e) $\frac{240\,018}{9\,900}$

c) $\frac{1\,462}{990}$ f) $\frac{1\,671}{99\,900}$

494. a) 2 b) 6 c) 16 d) 6

495. a) anteperíodo: 2; período: 1
b) anteperíodo: 1; período: 1
c) anteperíodo: 1; período: 6
d) anteperíodo: 1; período: 6
e) não tem; período: 6
f) anteperíodo: 1; período: 18

497. a) $n = 27k, 37k, 111k, 333k$ ou $999k$ ($k = 2{,}5$ ou 10)
b) $m = 47$

498. a) α c) $\beta = 3$

b) O pré-período de $\frac{1}{n^\beta}$ é β vezes o de $\frac{1}{n}$.

499. a) 11, 33 e 99
b) 101, 303, 909, 1 111, 3 333, 9 999

508. b) $p = 5, q = 3; |\sqrt{3} - \frac{5}{3}| \leqslant \frac{1}{12}$

c) $p = 3, q = 1; |\pi - \frac{3}{1}| \leqslant \frac{1}{6}$

d) $p = 8, q = 3; |e - \frac{8}{3}| \leqslant \frac{1}{15}$

BIBLIOGRAFIA

ADAMS, W. W. & GOLDSTEIN, L. J. *Introduction to number theory*. Prentice-Hall, Inc., 1976.
ANDREWS, G. E. *Number theory*. W. B. Saunder Company, 1971.
BATSCHELET, E. *Introdução à Matemática para biocientistas*. Editora Interciência / Edusp, 1978.
BOYER, C. B. *História da Matemática*. Editora Edgard Blücher / Edusp, 1976.
BURTON, D. M. *Elementary number theory*. Allyn and Bacon, Inc., 1980.
CARONNETH, TH. *Exercices d'Arithmétique*. Librairie Vuibert, 1955.
CATUNDA, O. *Curso de análise matemática* (cap. I). Editora Bandeirantes, 1953.
DOMINGUES, H. H. e IEZZI, G. *Álgebra moderna*. Atual Editora, 1982.
EVES, H. *An introduction to the history of Mathematics*. Holt, Rinehart and Winston, Inc., 1964.
GOFFMANN, C. *Introduction to real analysis*. Harper International Edition, 1969.
ITAR, J. *Les nombres premiers — Que sais-je?*. PUF, 1975.
KOULIVOK, L. *Algèbre et theorie des nombres*. Editions Mir, 1982.
MATEMÁTICA UNIVERSITÁRIA. Nº 1. SBM, 1985.
NIVEN, I. *Números: racionais e irracionais*. SBM, 1984. (Col. Fundamentos da Matemática Elementar.)
ORE, O. *Number theory and its history*. Mac-Graw Hill Book Company, 1948.
SHOCKLEY, J. E. *Introduction to number theory*. Holt, Rinehart and Winston Company, Inc., 1967.
SIDKI, S. *Introdução à teoria dos números*. IMPA, 1975.
VINOGRADOV, I. M. *Elementos of number theory*. Dover Publications, Inc., 1954.
VISWANATHAN, T. M. *Introdução a Álgebra e Aritmética*. Monografias de Matemática 33, IMPA, 1979.
VOROBYOV, N. N. *Los numeros de Fibonacci*. Editorial Limusa, 1973.

ÍNDICE REMISSIVO